(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 November 2001 (22.11.2001)

PCT

(10) International Publication Number
WO 01/088659 A3

(51) International Patent Classification[7]: G06F 17/00, 17/60, G06K 5/00, 7/01

(21) International Application Number: PCT/US01/15612

(22) International Filing Date: 15 May 2001 (15.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

09/571,707	15 May 2000 (15.05.2000)	US
09/619,859	20 July 2000 (20.07.2000)	US
09/667,835	21 September 2000 (21.09.2000)	US
09/667,081	21 September 2000 (21.09.2000)	US
09/667,039	21 September 2000 (21.09.2000)	US
09/667,082	21 September 2000 (21.09.2000)	US
09/667,038	21 September 2000 (21.09.2000)	US

(71) Applicant: **PRIVASYS** [US/US]; Suite 300, 40 First Street, San Francisco, CA 94105 (US).

(72) Inventors: **WONG, Jacob, Y.**; 7110 Georgetown Road, Goleta, CA 93117 (US). **ANDERSON, Roy, L.**; 1433 Dwight Drive, Glendale, CA 91207 (US). **BRYANT, William, R., Jr.**; 12001 Coverstone Hill Circle #324, Manasses, VA 20109 (US). **ZIEGLER, Joan, M.**; 2355 Paradise Drive, Tiburon, CA 94920 (US).

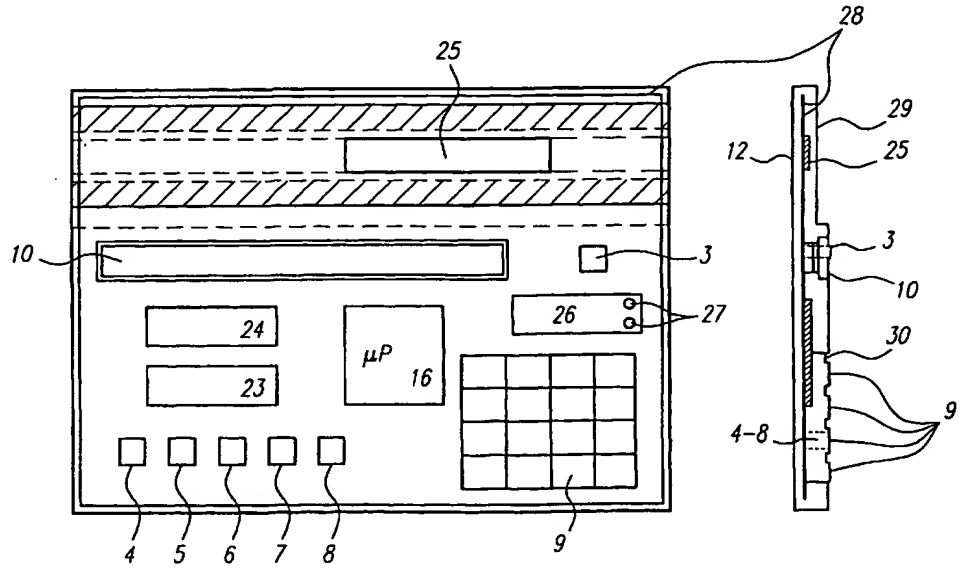
(74) Agent: **MCCONAGHY, John, D.**; Lyon & Lyon LLP, 633 West Fifth Street, 47th Floor, Los Angeles, CA 90071-2066 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian

[Continued on next page]

(54) Title: ELECTRONIC CARDS CAPABLE OF BEING READ BY A MAGNETIC STRIPE READER AND METHODS FOR THEIR USE



(57) Abstract: An electronic card that can function as an anonymous credit card or banking card for use on or off the Internet utilizes a magnetic storage medium 12 affixed to the card that can be read by a standard magnetic stripe reader. An encoder 25 generates a data packet that can be stored in a designated portion of the magnetic storage medium, which can be a magnetic stripe. The data packet can contain a personal coupon and an alias. A computer or microprocessor 16 generates the personal coupon after a Personal Identification Number is input into the card. The data packet can also be used to convey other information, such as a low battery condition. Several different methods of customizing use of the electronic card provide a vast array of options for handling multiple users, bills, accounts, and for characterizing individual transactions of the card.

WO 01/088659 A3

patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
18 April 2002

(48) Date of publication of this corrected version:
3 January 2003

(15) Information about Correction:
see PCT Gazette No. 01/2003 of 3 January 2003, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

procedures. As a result, many efforts, including several potentially promising efforts, have met with failure.

Even though new forms of electronic money have been slow to develop or gain widespread acceptance, electronic payments have still moved forward. Many banks now offer some form of electronic checking. And payment cards have been used for electronic transactions in e-commerce and m-commerce (mobile commerce). Still, there is widespread concern about the safety of such transactions, and recent news stories have uncovered widespread fraudulent activity associated with use of traditional credit card numbers in e-commerce over the Internet. In addition, there is growing concern about consumer privacy, or lack thereof, due to widespread electronic profiling of consumers who make electronic payments.

Although the media has been quick to cover fraud associated with use of credit cards over the Internet, it is often overlooked, at least by the public and the media (but not the credit card companies), that the majority of fraudulent activity concerning credit cards is not associated with e-commerce activity. Most fraud occurs in the "brick and mortar" world, and the numbers are daunting. Despite many attempts to combat unauthorized or fraudulent use of credit cards, it is estimated that credit card fraud now exceeds hundreds of millions, if not several billion, dollars per year. And this does not even count the cost of inconvenience to consumers, merchants and credit card issuer/providers, or the emotional distress caused to victims of such fraud, or the cost to society in terms of law enforcement and preventative activities.

Accordingly, there is a very real, long-felt need to reduce the amount of fraudulent activity that is associated with credit cards, and this need has only grown more acute as consumers and commerce search for better ways to purchase and sell goods and services via e-commerce and m-commerce. However, any solution needs to be something that is acceptable to the public at large. It should be easy to use. It should not be complicated or expensive to implement. Preferably, it should fit within the existing infrastructure, and not be something that requires a great deal of educational effort, or a radical change in behavior or habits of consumers. In other words, it should be user friendly, readily understandable and something that does not require a completely new

infrastructure, which is a reason suggested by some as to why smart cards have not been widely accepted in the United States.

In addition, it is highly desirable that any solution to such problems be capable of widespread use, in many different platforms, for many different applications.

In U.S. Patent No. 5,956,699 issued in September of 1999, Wong and Anderson were the first to introduce the methodology of a system for secure and anonymous credit card transactions on the Internet. This patent introduced a system which used an algorithm to use one's own selected Personal Identification Number or PIN as one's own de facto digital signature. The algorithm instructs the cardholder how to insert one's PIN into one's valid credit card number before using it for any transactions on the Internet. The resultant scrambled up credit card number, which is tailored by the algorithm to having the same number of digits as before, is rendered useless on the Internet because the PIN insertion algorithm is changed automatically after every transaction. This methodology is not only capable of drastically reducing credit card fraud on the Internet, it is also capable of safeguarding one's anonymity, and thus privacy, in credit card purchases on the Internet.

Since the issuance of U.S. Patent No. 5,956,699, Wong and Anderson have also invented an anonymous electronic card for generating personal Coupons useful in commercial and security transactions, as well as a method for implementing anonymous credit card transactions using a fictitious account name. The present invention is an extension of these prior inventions that seeks to provide new methods for allowing a user to customize the use of one-time unique numbers that can be used in credit card transactions in the brick and mortar world, e-commerce, m-commerce and in many other applications. Because the methodology is well suited for use in hardware and software applications, it has widespread applicability to many different types of transactions. In addition, the present invention allows a user to include data in the information that is transmitted as part of a normal payment card transaction. This allows the user a great deal of flexibility in customizing use of such a card. In addition, it allows a provider of the card to receive important information as part of the normal processing of a given transaction.

SUMMARY OF THE INVENTION

The present invention is generally directed to an electronic card that contains a magnetic storage medium, such as a magnetic stripe, and a mechanism for generating a data packet that can be read by a standard magnetic stripe reader. The electronic card also contains a card base, a computer or microprocessor, a display mechanism, an input mechanism and a power source. The present invention is also generally directed to methods for using such an electronic card. Such methods includes use of a data packet that can be read by a magnetic stripe reader and methods of customizing use of such a card, including customizing the use of an electronic card in financial transactions.

In another, separate aspect of the present invention, the data packet contains data representing a personal coupon and an alias that are readable by a standard magnetic stripe reader. The personal coupon and the alias can be used to conduct credit card transactions on or off the Internet. The data packet can also be used in a security device.

In other, separate aspects of the present invention, a computer in the electronic card executes a computer program, which can be a diagnostic program, to generate information that is stored in the data packet. An example of such a program is a program that checks on a battery life parameter. The program can generate a warning signal when a low battery condition is detected or a battery life signal related to an estimated remaining battery life of the battery. Such signals can be sent to the money source so that the user can be provided with a replacement electronic card either before or after the battery life drops below a selected threshold.

In still other, separate aspects of the present invention, a method for customizing payment card transactions is provided by allowing a user of a payment card to select a customization variable for any given transaction involving use of the payment card. The customization variable is submitted with the payment card number and a user identifier to a verification agency for validation. The customization variable may be used in a method for processing a plurality of payment card transactions based upon the user's selection of various customization variables. The present invention is particularly well suited for use

with electronic cards, but it can also be used in any method that uses a card number generator to generate a one-time card number.

The customization variable may involve customization of the generation of a one-time payment card number. An example of one way in which this can be done is to allow the user to choose either a first or a second user key as the key that will be used by an algorithm of a card number generator to generate the one-time payment card number. The customization variable may also involve customization of a user identifier associated with the one-time payment card number. An example of one way in which this can be done is to allow the user to choose either a first or a second identifier. The customization variable may also involve inclusion of a customization variable with the one-time payment card number and the user identifier when they are submitted to the verification agency for validation.

In still further, separate aspects of the present invention, multiple handling options provide numerous options for processing payment card transactions. The handling options can include billing two separate accounts. The user can be sent a single bill for charges to the two separate accounts, even if the accounts are established with different entities, such as different credit card companies or banks, or the user can be sent a first bill for the first account and a separate bill for a second account. One of the accounts can be a credit account and another account can be a debit account. The handling options can provide a mechanism for classifying the nature of the payment card transactions, such as using a first handling option for business transactions and a second handling option for personal transactions. They can also provide different mechanisms for controlling access to information concerning payment card transactions. One mechanism can be used to implement restrictions on distribution of information relating to payment card transactions or restrictions on distribution of personal information of the user to second entities. The user can be charged consideration for use of this mechanism. Another mechanism can be used to permit distribution of information relating to payment card transactions to third parties or permit distribution of personal information of the user to second entities. The user can be given consideration to use this mechanism.

In yet other, separate aspects of the present invention, a method is provided for delivery of an item purchased through a secure and anonymous transaction between a user and a merchant with subsequent. The user selects a customization parameter at the time of purchase that is used to implement an anonymous delivery method. The customization parameter can be used to customize generation of a user-one time payment card number, a fictitious user identifier or as a customization variable included with the user one-time payment card number and the fictitious user identifier in a transaction data packet provided by the user to the merchant, and ultimately to the money source. After the money source confirms that the transaction is valid and that the user has elected an anonymous delivery option, the money source sends a tracking identifier to the merchant and a delivery agent. Next, the merchant delivers the purchased goods to the delivery agent, and the delivery agent delivers the purchased goods to a delivery address provided by the money source. The merchant need not ever be provided with the delivery address, and the delivery agent need not ever be provided with any details concerning the goods or the transactions.

Accordingly, it is a primary object of the present invention to provide an electronic card that can be used for commercial and security transactions in which an input is needed to control the function of the card and methods for using such cards.

This and further objects and advantages will be apparent to those skilled in the art in connection with the drawings and the detailed description of the preferred embodiment set forth below.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a physical layout of a preferred embodiment of a Universal Anonymous Credit Card (UACC) in accordance with a preferred embodiment of the present invention.

Figure 2 is a system block diagram of a preferred embodiment of the Universal anonymous Credit card (UACC) in accordance with a preferred embodiment of the present invention.

Figure 3 is a physical layout of a preferred embodiment of the Universal anonymous Credit Card (UACC) in accordance with a preferred embodiment of the present invention.

Figure 4 shows an un-coded magnetic stripe likened to a series of aligned South-North magnetic domains.

Figure 5 shows a sudden introduction of a strong magnet having an opposite orientation on top of a magnetic domain of the magnetic stripe causing flux reversals.

Figure 6 shows flux reversals caused by sudden introduction of strong magnet having opposite magnetic orientation on top of a magnetic domain in a magnetic stripe.

Figure 7A is an un-coded portion of a track of a magnetic stripe having 5 bit cells showing no flux reversals.

Figure 7B shows a representation of all "0", all "1" and "0" and "1" side by side according to the Aiken Biphase encoding code.

Figure 7C shows a representation of decimals "0", "5" and "9" in the Aiken Biphase encoding standard.

Figure 7D shows a preferred embodiment of an encoder head of the present invention.

Figure 8 shows a preferred embodiment of an encoder of the present invention with drive electronics and logic.

Figure 9 is a simplified, schematic diagram of a preferred method of using an electronic card in a financial transaction.

Figure 10 is a physical layout of a front-side of an alternate preferred embodiment of a Universal Anonymous Credit Card.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

1. A preferred embodiment of an electronic card

In a preferred embodiment of the present invention, a unitary, self-contained electronic device is provided having physical planar dimensions that are essentially identical to those of a conventional magnetic stripe credit card, which is widely used in electronic commerce today. The device has several components,

although some components can be combined together or omitted from some embodiments.

An initial component is the card base. The other components, in one way or another, are attached to this base.

Another component is a computer or microprocessor. It is preferable that the computer be a single integrated chip, but it need not be. A computer typically contains a central processing unit connected to both storage memory and random access memory (RAM). RAM is used to load and run application programs as well as for storing data during run time. The storage memory can hold a variety of computer programs.

Still another component is a display controlled by the computer. In one preferred embodiment, this is a liquid crystal display (LCD). The LCD can be controlled by a LCD driver, and the LCD driver can be contained in storage memory of the computer. In an alternative embodiment, the display is a series of light-emitting diodes, each of which is associated with a numeric key of a keypad. In still another alternative embodiment, the display can be an electronic ink display, which is a novel and newly available display medium. The electronic ink display can be fabricated with highly flexible physical dimensions, especially in thickness, which is likened to a thin piece of paper and also much cheaper to manufacture than conventional LCD display.

The card must also have an input mechanism. In the preferred embodiment, this is a keypad. However, it is possible that the input mechanism might rely upon voice recognition as this technology becomes more and more developed.

The card also has a magnetic storage medium, which, as already noted, is a magnetic stripe in an especially preferred embodiment.

The card also has a mechanism for generating a data packet. In a preferred embodiment, an encoder is used to generate a data packet that is stored in a designated portion of the magnetic storage medium. This component allows the electronic device to be dynamic by relying upon an input to generate the data packet.

Finally, the card has a power source. In the preferred embodiment, this is a battery or a solar cell.

1.1 Use of the preferred embodiment in a credit card

The electronic card just described can be used in a method for implementing an anonymous credit card transaction between a user and a merchant. A preferred embodiment of such a method is depicted in Figure 9. In accordance with this preferred embodiment, a user must first establish a user account with a credit source. The credit source may be a bank, a credit card company or any other institution involved with issuance of credit cards or bank debit cards, such as a credit union or other institution, or a money source as described in U.S. Patent No. 5,913,203. When the user establishes a user account with the credit source, one or more user settlement mechanisms through which the user can pay the credit source for charges and fees billed to the user account will be established. For example, in the case of credit card transactions, the user and the credit source will enter into an agreement concerning use of the credit card. As a further example, in the case of debit or electronic checking services, the user and credit source may enter into a separate agreement concerning how and from what account such debits will be debited.

After a user account is established, the credit source will create one or more user account records associated with the user account to contain a variety of information including a user account number, a fictitious account name, a "Proxy Agent," a user key and, when applicable a user insertion key. The fictitious account name can be selected by the cardholder or the issuer of the credit card, but it has to be known by both. The "Proxy Agent" is used to conceal the cardholder's actual address and still comply with current credit card regulations – in other words, it is a fictitious address. Additional information that might typically be contained within such records includes cross references to other accounts, the user's name and the user's billing address.

One function of this electronic credit card, which shall be referred to as the Universal Anonymous Credit Card (UACC), is to allow a credit cardholder to execute secure and anonymous credit card transactions on and off the Internet. This can be done in a system and in methodology in which merchants no longer have access to the cardholder's real name, address and the actual valid credit card number. Such an effectual personal encryption does not, however, prevent the additional use of an Internet standard encryption such as SSL or SET for

online data exchanges. The latter will simply make such online transactions even more secured.

For purposes of clarification and illustration, an example of an application that uses the methodology taught in U.S Patent No. 5,956,699 is presented here. Assume that the card number (CN) stored in the electronic card and the PIN number are, respectively:

CN = 4678 0123 4567 8012 1200

PIN = 2468

Next, assume that the application uses an algorithm that first deletes four (4) digits from the CN and then inserts in their place the PIN according to the insertion sequence indicated by a so-called PIN Sequence Insertion Number (PSIN) in order to come up with a scrambled Anonymous Credit Card Number (ACCN), also containing 20 digits. The 4-digit PSIN number can either be chosen by the cardholder or assigned by the issuer. Let us assume for this example that the cardholder's PSIN is 1357.

Next, assume that the algorithm only operates on digits 7 through 16 of the CN. This takes into account the fact that the first 4 digits of the standard CN denote the identification of the credit card issuer and the last 4 digits of the standard CN are reserved for the expiration date, all of which should be left undisturbed. Thus, it is the middle 11 digits that indicate the account number for the cardholder of the CN. Therefore, the algorithm calls for the cardholder to first delete the last four digits of the 10-digit account number. In this example the 4 digits to be deleted will be "8012". The 6-digit number before the cardholder PIN is inserted according to the cardholder's PSIN is "23 4567".

Now the algorithm defines the numbering convention of the digit positions in the ACCN. The first digit position is defined as the zeroth (0^{th}) and the second is the first (1^{st}) etc. Thus, according to the PISN 1357, the PIN 2468 should be inserted to form the ACCN as follows:

ACCN = 467801 2<u>2</u>3<u>4</u>4<u>6</u>5<u>8</u> 671200

The 4 digits of the PIN= 2468 occupy, respectively, the 1^{st}, 3^{rd}, 5^{th} and 7^{th} positions (according to PISN=1357) using the defined digit position numbering convention. In a simpler algorithm for inserting the PIN, the PIN number itself can act

effectively as the PSIN so that the cardholder does not have to remember two numbers. Using such an algorithm, in the example above, the ACCN will now be:

ACCN = 467801 2324456687 1200

The 4 digits of the PIN = 2468 also occupy, respectively the 2nd, 4th, 6th and 8th positions of the ACCN (according to an implicit PSIN = PIN = 2468) using the defined digit position numbering convention.

The foregoing is an example of a very simple algorithm to generate a valid personal charge number. As would be apparent to a person of ordinary skill in the art of computer programming, especially with the benefit of this disclosure, much more complicated algorithms could be devised and used which would use the card number and the user key to generate a valid personal charge number.

The applications just described can be used in a system that reduces fraud while protecting consumer privacy through anonymous transactions, on and off the Internet. Such a system has three main components that are provided to complete a commercial credit card transaction. First, instead of using a valid credit card number, an ACCN is used. Second, instead of using the cardholder's real name, an alias is used. The alias can be selected by the cardholder or the issuer of the credit card, but it has to be known by both. Third, instead of using a cardholder's real address, a "Proxy Agent" is used to conceal the cardholder's actual address and still comply with current credit card transaction regulations. In such a system, the use of a credit card for transactions on the Internet can be anonymous to all except the cardholder and the credit card issuer.

When the electronic card is used in a retail transaction, by merely entering one's own PIN into the electronic card prior to giving it to the merchant for swiping the credit card transaction, one takes full advantage of the secure and anonymous transaction afforded by the electronic card. The user can first check his or her alias and entered PIN (note that the PIN is not stored in the electronic card) using the keypad on the electronic card before the electronic card is handed over to the merchant. Since the cardholder has in effect already signed the transaction with a digital signature (his or her PIN), no additional hand signature is required to complete the transaction. The merchant only need receive the PIN-modified anonymous credit card number (ACCN) and the user's alias. The ACCN and the aliases are read by a conventional magnet stripe reader and are processed in

exactly the same fashion as a conventional credit card number and credit cardholder name since such information can be sent to a credit card approval agent for approval of the transaction. The credit card approval agent has all of the information necessary to determine if the transaction is valid or fraudulent. The identity of the entity who authorized the credit card, as well as its expiration date, is available in the ACCN in just the same manner as it is available in a conventional credit card transaction. The card number is verified by confirming the card number contained in the ACCN as valid for the alias.

To use the electronic card for Internet transactions, a cardholder first enters the PIN into the electronic card exactly like that for off the Internet transactions. Next, the cardholder continues the transaction using only the cardholder's alias, the ACCN appearing in the LCD display and also the cardholder's choice of trusted delivery or Proxy Agent (optional) should the cardholder prefer to make this transaction completely anonymous. Thus, by carrying just one electronic card which looks and feels exactly like a regular magnetic stripe credit card, one is now able to make old world credit card transactions like one always has done in the past. But more importantly, one can now use the same electronic card for making secure an anonymous transaction, anywhere in the world, and for both on and off the Internet transactions.

As is apparent from the foregoing description, the real name and address of the cardholder, including the credit card number itself, never need appear on the Internet or even need to be made known to the merchant. Even though the ACCN or Coupon (Customer One-time Unique Purchase Order Number) does appear, together with the alias of the cardholder, across the Internet during the online transaction, this ACCN or Coupon number does not stay the same, but changes automatically after every transaction or use. Thus, no valid credit card numbers are actually available in transmission for theft by anybody. Only the ACCN or Coupon number will appear on any or all transaction records and that number is useless for subsequent transaction because it is time variant.

1.2 Additional details regarding construction of one preferred embodiment of an electronic card

In order to reduce the cost of use of the UACC, and increase the range of applications in which it can be used, the UACC should have a magnetic storage

medium that can be read by a standard magnetic stripe reader. This means that the magnetic storage medium must be capable of being read by a standard magnetic stripe reader. It also means that the portion of the UACC containing the magnetic storage medium must be sized such that the magnetic storage medium will work with standard magnetic stripe readers. A standard magnetic stripe reader works by passing the magnetic stripe portion of a card, such as a credit card, through the magnetic stripe reader in a swiping motion. Standard magnetic stripe readers have been prevalent in retail stores throughout the United States for many years.

An especially preferred embodiment of the present invention will now be described in even greater detail. The especially preferred embodiment uses a standard microprocessor having its usual Central Processing Unit (CPU), Read-Only-Memory (ROM), Random-Access-Memory (RAM) and Input-Output devices (I/O). There are two types of ROMs in the UACC. The first type is a standard semiconductor ROM, ROM1, fabricated as part of the microprocessor. ROM1 stores the microprocessor operating system and also the bulk of the methodology software. The second type of ROM, ROM2, is a portion of a magnetic stripe, namely Tracks 1 and 3. ROM2 stores the relevant information about the cardholder such as primary account number VCCN, name, expiration date, encrypted PIN etc. There are also two types of RAMs in the UACC. The first type of RAM, RAM1, is a standard semiconductor RAM as part of the microprocessor and needed for its normal operation. The second type of RAM, RAM2, is a portion of a magnetic stripe, namely Track 2. RAM2 temporarily stores the encoded ACCN to be read by a standard magnetic stripe reader during a normal credit card transaction after the cardholder inputs the PIN according to the PSIN algorithm into the UACC.

The methodology software is installed into ROM1 of the microprocessor during production. A standard parallel port Input Device serves to interface a numeric keypad and other functional switches of the UACC to the microprocessor. The UACC also has two Output Devices. The first Output Device is a standard parallel output port of the microprocessor used for interfacing to it a 10- or more character alphanumeric LCD display through a driver for outputting information such as recalling from memory alias or typed in PIN verification. It is also used for

production testing and repair or servicing of the UACC. The second Output Device is an integrated circuit (IC) magnetic encoder unit built into the UACC so as to encode Track 2 of the magnetic stripe or RAM2, either statically in conjunction with the existing magnetic stripe, or dynamically without the use of the existing magnetic stripe, with the temporary ACCN information for off the Internet credit card transactions. In this especially preferred embodiment of the present invention illustrated below, only the static magnetic encoder working in conjunction with the existing magnetic stripe is described in detailed. For those skillful in the art, the dynamic thin film magnetic encoder, working without the use of the existing magnetic stripe, can also be used in the present invention as an alternative embodiment. In a preferred embodiment of the present invention, the UACC also contains a battery cell, ON/OFF and other functional switches to render it a fully functional and self-contained credit card (see Figure 1).

The UACC bridges the old economy world of brick and mortar to the new economy world of the Internet. The integrated circuit (IC) magnetic encoder with current-carrying conductive writing heads is fabricated on a flexible and ultra-thin polymer (e.g. polyimide) printed circuit board (PCB) intimately in contact with the magnetic stripe located above for data impression. The encoder driver and digital logic chips are also mounted on the flexible PCB, but in different areas to form the complete IC magnetic encoder. The IC magnetic encoder is technically compatible with conventional magnetic data transfer methodology and makes possible the fabrication of the present UACC with physical dimensions exactly like those for a regular magnetic stripe portion of a credit card.

Even greater detail will now be provided by reference to Figures 1 through 8.

Figure 1 shows the physical layout for an embodiment of the present electronic device or Universal Anonymous Credit Card (UACC) 1. The areal dimensions of the UACC 1are 3.375" x 2.125" or exactly those of a regular magnetic stripe credit card in use in electronic commerce today. The thickness of the UACC 1 varies from ~0.030" at the top where the magnetic stripe resides to 0.030" – 0.060" for the rest of the card dependent upon the thickness of the LCD used (see Figure 1). Besides the ON/OFF switch 3, the front side 2 of this UACC 1 has five (5) more functional switches, 4-8, labeled and defined as follows:

ATM (switch 4) = Reserved for Automatic Teller Machine (ATM) card

ACC (switch 5) = Reserved for Anonymous Credit Card (ACC or A-Card)

IC (switch 6) = Reserved for Internet Type II Cash

MC (switch 7) = Reserved for standard Magnetic Stripe Credit Card

BC (switch 8) = Reserved for A-Card transactions using bar codes

In addition to the switches 3 – 8, there is a 12-character keypad 9. The primary function of the keypad 9 is for the cardholder to enter the PIN into the UACC 1 for generating the ACCN for on and off Internet commerce transactions. There is also a 10- or more character alphanumeric liquid crystal display (LCD) 10 on the front side 2 of the UACC 1. This LCD 10 displays the alias and the ACCN for use for Internet commerce transactions or the alias and bar code representing the ACCN after the cardholder's PIN is entered. The display of the ACCN will automatically erase itself after about 2 minutes to avoid exposing significant information to third parties.

At the top of the back side 11 of UACC 1 is a standard 3-track magnetic stripe 12 found in every common magnetic stripe credit card in use today. Track-1 13 and track-3 14 are used to store the relevant information about the cardholder such as primary account number VCCN, name, expiration date, encrypted PIN etc. Track-2 15 of the magnetic stripe 12 normally contains only the cardholder's VCCN to be read by a magnetic stripe reader at the merchant's site. For the present UACC device, the ACCN, instead of the VCCN, will be generated on command by entering the PIN with the appropriate function switch "MC" 7 by a special encoder 16 located at a designated location underneath the magnetic strip 12. As will be explained in more detail below, the generated ACCN which resides temporarily on Track-2 15 of the magnetic stripe 12 will disappear automatically 2 minutes after it is being generated. This is to ensure that no significant information about the credit card account stays long enough for someone to steal for committing subsequent credit card frauds.

The system block diagram for the especially preferred embodiment of the present invention is shown in Figure 2. At the center of the system is a conventional 16-bit microprocessor 16 comprising a Central Processing Unit (CPU) 17, a Read-Only-Memory (ROM1) 18, a Random Access Memory (RAM1) 19, a 16-bit parallel Input Port (Input) 20 and a 16-bit parallel Output Port (Output)

21. The microprocessor 16 receives inputs through Input 20 from a bank of functional switches 22, which contains switches 4 through 8. The microprocessor also receives inputs from a 12-character keypad 9 through Input 20. Outputs from the microprocessor 16 emanate from Output 21 through a LCD display driver 23 to reach the 10- or more character alphanumeric LCD display 10 and also through an encoder driver 24 to reach a designated location of Track-2 15 of the magnetic stripe 12. Such a designated location of Track-2 15, where the encoder 25 is positioned, serves as a second RAM, RAM2, for the microprocessor 16. RAM2 stores the encoded ACCN needed for offline credit card transactions to be read by the merchant's standard decoding equipment very much like a conventional magnetic stripe credit card.

The software program is installed into ROM1 18 of the microprocessor 16 during production of the current UACC unit. Information pertaining to the cardholder is encoded onto Track-1 13 and Track-3 14 of the magnetic stripe 12 which serves as an independent ROM, ROM2, for the UACC unit. Since information stored in ROM2 will be read with a standard magnetic stripe reader, it operates independently of the microprocessor 16. A battery supply 26 with contacts 27, controlled by the ON/OFF switch 3, completes the UACC system. The battery supply provides power to all the components of the UACC system, including the microprocessor 16, LCD display driver 23, encoder driver 24, LCD display 10 and the keypad 9.

Figure 3 shows the physical layout and construction for the especially preferred embodiment of the present UACC device. All the electronic components of the system, namely the microprocessor 16, the LCD display 10, the keypad 9, LCD display driver 23, encoder driver 24, encoder 25, functional switches 4-8, ON/OFF switch 3 and battery contacts 27 with battery cell 26, are fabricated on a flexible multi-layered printed circuit board 28. The flexible printed circuit board 28 with all the loaded components is then encapsulated in plastic into thin 29 and thick 30 parallel sections as shown in Figure 3. The thickness of the thin section 29 where the conventional magnet stripe 12 will be fabricated on top of the encoder 25 (to be explained in more detail below) on the backside is about 0.030", the same thickness as the magnetic stripe credit cards in use today. The plastic encapsulated thick section 30 (see Figure 3), while holding the fully-loaded flexible

printed circuit board 28 in place, allows the ON/OFF switch 3, functional switches 4-8 and the keypad 9 to be physically accessible (e.g. by fingers) from the front side of the UACC device. The LCD display 10 is also directly visible from the front side. Note that the thickness of the plastic encapsulated section would also be 0.030" thick if a polymer-backed (e.g. Mylar®) ultra-thin LCD display (0.020" thick typical) is used.

1.2.1 Background discussion of magnetic stripe technology theory

A much simplified theory on magnetic stripe technology, especially on how to encode (write) and decode (read) digital data respectively on and off a magnetic stripe used in ordinary credit cards of today, will now be provided in order to better explain one way in which an encoder can be fabricated and work. A magnetic stripe is made out of a thin layer of very tiny ferromagnetic particles (typically 0.5 micron long) bound together with resin and subjected to a very strong magnetizing magnetic field (known as "coercivity") when such a stripe is printed onto a substrate. When the resin is cured or set, these tiny "magnets" are magnetically and permanently aligned (magnetized) into a series of South-North magnetic domains forming a chain of S-N, S-N ... interfaces. The adjacent N-S magnetic fluxes of these magnetic domains are normally linked together for the entire magnetic stripe to act like a single magnet with South and North poles at its ends. In other words, an un-encoded magnetic stripe is actually a series of aligned South-North magnetic domains (see Figure 4).

If a N-N interface (instead of the normal N-S interface for un-encoded magnetic domains) is created somewhere on the stripe, the magnetic fluxes at the N-N interface will repel each other, resulting in a concentration or increase of flux lines around the N-N interface called a "flux reversal". The same situation exists for a S-S interface as compared with a normal N-S interface. Such a situation will take place if a strong magnetizing magnet 31 having an opposite magnetic orientation, namely N-S, is suddenly introduced on top of one of the S-N magnetic domains 32 of the magnetic stripe as shown in Figure 5. The magnetic domain 32 will realign its magnetization as that of the strong magnet on top of it, namely N-S. Under this situation, two flux reversals have taken place, as illustrated in Figure 6.

The process of encoding or writing involves the creation of N-N and S-S magnetic domain interfaces, or flux reversals, and the process of decoding or

reading that of detecting them. Knowing that magnetic flux lines always emanate from the North pole and terminate on the South pole, a sudden introduction of a strong magnetic field (greater than the coercivity of the magnetic domains) having a N-S magnetic orientation can magnetize a normal S-N magnetic domain into N-S orientation, resulting in the creation of a pair of flux reversals S-S and N-N, much like that shown in Figure 6 above.

Before proceeding to explain how the encoder of the especially preferred embodiment writes the ACCN on Track-2 15 of the magnetic stripe 12, it is helpful to delve deeper into the data storage mechanics of the magnetic stripe 12 itself. As stated earlier, the magnetic stripe 12 has three tracks, namely Track-1 13, Track-2 15 and Track-3 14. Digital data are stored in these three tracks according to the American National Standards Institute (ANSI) and International Standards Organization (ISO) BCD (5-bit Binary Coded Decimal Format) or ALPHA (alphanumeric) standards. The ANSI/ISO standards for Tracks 1, 2 and 3 are summarized in Table I as follows:

Table I. ANSI/ISO Track 1, 2, 3 Standards

Track	Name	Density	Format	Characters	Function
1	IATA	210 bpi	ALPHA	79	Read Name & Account
2	ABA	75 bpi	BCD	40	Read Account
3	THRIFT	210 bpi	BCD	107	Read Account & Encode

Track-1 13, named after the "International Air Transport Association" (IATA), contains the cardholder's name as well as account and other discretionary data. Track-2 15, "American Banking Association" (ABA), is the most commonly used. This is the track that is read by ATMs and credit card checkers. The ABA designed the specifications of this track and it is believed all major world banks abide by it. It contains the cardholder's account number, encrypted PIN, plus other discretionary data. Track-3 14 is unique and intended to have data read from and written on it. At present, it is an orphaned standard and has not been widely used to date.

Before the encoder can write on command the ACCN on Track-2 15 of the magnetic stripe, attention must be paid to the data layout for Track-2 15.

Encoding protocol specifies that each track must begin and end with a length of all Zero bits, called CLOCKING BITS. These are used to synchronize the self-clocking feature of bi-phase decoding, an industry standard. A typical Track-2 layout is shown as follows:

0000000000000000 ; 1111222233334444=9912****000000XXXX0000?

The symbol ";" after the "0's" is the "START SENTINEL" according to the BCD data format. The 4 digits "1111" following is the issuer or acquiring bank's identification number. The 12 digits following is the cardholder's account number. The symbol "=" following is the "FIELD SEPARATOR" according to BCD data format. The 4 digits "9912" following is the expiration date. The four characters following "****" are data reserved for private use. The data length "XXXX" after the string of 0's may vary and is the encrypted PIN offset. Finally the symbol "?" after another string of 0's is "END SENTINEL".

The location of the 12 digits that need to be encoded or written on command is represented by "2222 33334444" on Track-2 15 of the magnetic stripe 12 in the example cited above.

Next, it is helpful to have an understanding of how the 12 digits are represented in BCD data format on Track-2 15 of the magnetic stripe 12. According to the BCD data format, each decimal digit is coded by 5 bits. The ANSI/ISO BCD Data Format is reproduced in Table II below. Note that all 21 digits, including the field separator, namely "1111222233334444=9912", can also be encoded on command if so desired.

Table II. ANSI/ISO BCD Data Format

Data Bits				Parity	Character[1]	Function
b1	b2	b3	b4	b5		
0	0	0	0	1	0 (0H)	Data
1	0	0	0	0	1 (1H)	Data

0	1	0	0	0	2	(2H)	Data
1	1	0	0	1	3	(3H)	Data
0	0	1	0	0	4	(4H)	Data
1	0	1	0	1	5	(5H)	Data
0	1	1	0	1	6	(6H)	Data
1	1	1	0	0	7	(7H)	Data
0	0	0	1	0	8	(8H)	Data
1	0	0	1	1	9	(9H)	Data
0	1	0	1	1	:	(AH)	Control
1	1	0	1	0	;	(BH)	Start Sentinel
0	0	1	1	1	<	(CH)	Control
1	0	1	1	0	=	(DH)	Field Separator
0	1	1	1	0	>	(EH)	Control
1	1	1	1	1	?	(FH)	End Sentinel

Note 1. Hexadecimal conversions of the data bits are given in parenthesis (xH).

How BCD data is actually encoded onto Track-2 15 of the magnetic stripe 12 can now be explained. Table I above notes that Track-2 has a density of 75 bits per inch (bpi). According to the ANSI/ISO BCD data format, each character is represented by 5 bits. Thus, if the encoder needs to encode 12 digits (see "222233334444" in example above), it will require a total of 60 bits. Since the density is 75 bpi, the maximum physical space available for a stationary encoder head is 0.800". But the important dimension for the design of the encoder head is the space available for each BCD bit. In the present case, the bit dimension is 1,000 mils/75 bits or 13.33 mils (0.0133") per bit.

At this point, it is useful to explain with the help of Figures 7 A-D, how a single character or decimal digit comprising 5 bits in the ANSI/ISO BCD data format is encoded onto Track-2 15 of the magnetic stripe 12. Figure 7A shows an un-encoded strip of Track-2 long enough to accommodate 5 bits of data. The physical length of this strip is 5 x 0.0133" or 0.0667" (66.65 mils). This un-encoded strip is divided into five segments, each representing a single bit, and each is further represented by two magnetic domains as shown in Figure 7A. In

accordance with the industry standard of encoding called Aiken Biphase, or "two frequency coherent-phase encoding", data is encoded in "bit cells" defined above and the frequency of which is the frequency of the '0' signals. '1' signals are exactly twice the frequency of the '0' signals. So, at least from the conventional way of decoding, the actual frequency of the data passing the 'READ' head will vary with the swipe speed, for the data density, control functions etc., the '1' frequency, however, will always be twice the '0' frequency. This is illustrated in Figure 7B where the representation of all '1s' , all '0s' and how '1' and '0' data exist side by side. Note that in Figure 7B, the bit cell waveforms for '0' and '1' are the results of creating the so-called flux reversals of "N-N" or "S-S" at the magnetic domains interfaces of the un-encoded strip. For the stationary encoder of the present preferred embodiment, the encoding must be consistent with the Aiken Biphase convention because the same 'READ' heads will be used to decode the Track-2 data temporarily stored in UACC devices during offline (off the Internet) credit card transactions.

Consistent with the Aiken Biphase convention therefore, Figure 7C shows, as an illustration, how BCD decimal digits '0', '5' and '9' would appear referenced to the un-encoded 5-bit strip of Figure 7A. Also shown in Figure 7C are the orientation of the magnetic domains and the flux reversals at the domain interfaces. Thus, if an encoder head of the present preferred embodiment is designed to be on top of the 10 magnetic domains representing the 5-bit decimal digit, it would be possible to magnetize on command the individual domains in order to create the appropriate flux reversals corresponding to the desired decimal digit. This is illustrated in Figure 7D. The orientation of the magnetic domain 33 when un-coded is S-N as shown in Figure 7D. The two contact bits 34 and 35 control which direction the magnetizing current is flowing. When 34 and 35 are suddenly made "1" and "1", current I+ will flow in from contact 34 to ground resulting in flipping the orientation of magnetic domain 33 to N-S. Meanwhile the current I- from "+V" to contact 35 is zero. When contact 34 and 35 are suddenly left open circuited, both I+ and I- are zero and the orientation of magnetic domain 33 will stay as N-S. When contacts 34 and 35 are suddenly changed to "0" and "0", current I- will flow from "+V" to contact 35 and cause the magnetic domain to revert back to S-N while I+ is zero. No domain flipping occurs if the bits for

contacts 34 and 35 are either "1" "0" or "0" "1". In the former case, the magnetizing effect of I+ is neutralized by I-. Both I+ and I- are zero for the latter case. The magnitudes of currents I+ and I- needed to flip the magnetic domains with coercity of the order of 300-500 gausses ("soft" magnetic stripe found in conventional credit cards) for current carrying conductor of 1-2 microns thick are several hundred milliamperes. The electrical power required to encode or decode 12 decimal digits is of the order of tens microwatts.

In order to encode in the present example a total of 12 decimal digits, one would need to encode 5 x 12 or 60 bits of data. As shown in Figure 7D, the encoder has to have two micro-heads per bit of data. Furthermore, each micro-head has a PLUS or MINUS polarity. If the polarity is PLUS, current will flow in one direction so as to generate a N-S magnetizing magnet. Similarly, if the polarity is MINUS, current will flow in the opposite direction so as to generate a S-N magnetizing magnet. So the encoder of the present preferred embodiment will have 2 x 60 micro-heads each with a PLUS and MINUS polarity. An especially preferred embodiment of the encoder with the driver electronics and logic is shown schematically in Figure 8.

Figure 8 shows the 12 decimal digits divided up into 60 bit cells with each bit cell comprising two magnetic domains and each having a PLUS and MINUS polarity. There are therefore a total of 120 magnetic domains that have to be addressed, each with two polarities, making it a total of 240 address lines as shown in Figure 8. These addresses lines are accessed in bunches of 10 (5 magnetic domains or 21/2 bit cells). The address originates from using 10 bits of the 16-bit Output port 21 (see Figure 2 of system block diagram for UACC) and then through the encoder driver 24 (also see Figure 2) as current buffer before being connected to the 24 bunches of 10 address lines. Each of the 24 bunches of 10 address lines is accessed with a 32:1 decoder using five of the 16 bits of the Output parallel port 21. The decoder selects one of the 24 bunches of 10 address lines via switch bank 36 (there is a total of 24 switch banks similar to switch bank 36) comprising 10 switches each. In essence, it is the switch bank that selects which of the 10 address lines out of the 24 bunches that are being connected to the output of the encoder driver 24. Thus, it is possible to encode the 12 decimal digits into a designated location of Track-2 15 of the magnetic stripe with

commands from the microprocessor and outputted through the parallel port 21 through the encoder driver 24. Such a software command is stored in ROM1 (see Figure 2) of the microprocessor 16. The stored algorithm generates the ACCN or, in essence, a "Coupon" (Customer's one-time unique purchase order number), from the valid credit card number VCCN and the cardholder's PIN when inserted properly into part of the VCCN.

1.3 Additional details regarding use of the Universal Anonymous Credit Card

The manner in which the Universal Anonymous Credit Card (UACC) will work under different on and offline transaction circumstances will now be described in greater detail. It is first assumed that the cardholder has opened an UACC account with an issuer or acquiring bank. The cardholder has turned over a real name, address, personal and financial information to the issuer. In return, the cardholder is assigned a valid credit card number, VCCN, a credit limit, an Alias (chosen by the cardholder) and a proxy agent, and most importantly a cardholder UACC. The issuer has to assign the cardholder a proxy agent to use instead of giving out the cardholder's address in order to comply with the existing credit card transaction regulation. After obtaining a UACC from the issuer, the cardholder is now free to do anything and everything on and off the Internet safely with full assurance that nobody will find out what, where, when and how money is being spent with the UACC card, except its issuer.

The manner in which the cardholder can use his or her UACC to shop on the Internet will now be described. It is possible that not every online merchant will accept the UACC in the beginning, so the cardholder may have to identify those merchants that are partners with the UACC issuer bank. Otherwise, the transactions with the UACC will not be processed properly by the existing infrastructure that processes only conventional credit cards. Suppose the cardholder now wishes to purchase some merchandise from an online merchant who accepts UACC. All the cardholder has to send to the merchant's Web site online is his or her alias, a proxy agent's name assigned to the cardholder by the issuer bank, the ACCN or anonymous credit card number which will be obtained from the UACC (to be explained below), the merchandise and shipment choice. This is completely different from what the cardholder normally has to give out, viz.

a real name, address and the valid credit card number, should the cardholder use a regular credit card. To obtain the ACCN from his UACC device, all the cardholder has to do is to first push the button "CC", which is reserved for Anonymous Credit Card transactions, then to enter the cardholder's PIN using the keypad and then the "#" key. In the LCD display, the alias will first be scrolled across the display followed by the 10-digit ACCN. Note that the first six digits (four digits are used to identify the issuer bank and two more digits to designate a specific BIN number) and the last four digits of the ACCN always remain the same as those in the VCCN which signifies the issuer's identification and credit card BIN number, and the expiration date respectively. The cardholder can then use this ACCN to complete the transaction with the online merchant. After the cardholder finishes using the ACCN, he or she can either erase it from the LCD display by pressing "*" followed by "#" in the keypad, otherwise the ACCN will disappear from the LCD display automatically after approximately 2 minutes.

As one can see from this transaction on the Internet using the UACC, the real name and address of the cardholder, including the credit card number itself, never appear on the Internet or even are made known to the merchant. Even though the ACCN or Coupon does appear, together with the alias of the cardholder, across the Internet during the online transaction, this ACCN or Coupon number does not stay the same, but changes automatically after every transaction or use. Thus, unlike all the other credit card transactions on the Internet today, no valid credit card numbers are actually available in transmission for theft by anybody. Only the ACCN or Coupon number will appear on any or all transaction records and that number is useless for any subsequent transactions because it is time variant.

For off the Internet transactions, the UACC behaves just like an ordinary credit card. The only difference is that before one hands over the UACC to the merchant for charging the amount, one enters one's PIN after pushing first the "MC" button on the UACC device, which is reserved for magnetic stripe credit card transactions, and then follows it with a "#" key on the keypad. It is assumed here that the cardholder is satisfied with what is being charged on the credit card before the cardholder, in effect, "signs" it digitally in the transaction. Unlike ordinary magnetic stripe credit cards of today, no personal hand signature is

needed for off the Internet transactions with the UACC. By entering the PIN, the UACC automatically encodes temporarily the ACCN onto Track-2 of the magnetic stripe 12. The use of the resultant ACCN or Coupon is likened to the cardholder already signing the credit card with a personal digital signature for the transaction. The rest of the transaction simply follows that of a regular magnetic stripe credit card with the existing credit card processing infrastructure.

2. An alternative preferred embodiment of an electronic card

Another preferred embodiment with an alternative structure will now be described. In this embodiment, which is depicted in Figure 9, the electronic card does not have a display, such as the LCD; instead, the keypad has LEDs associated with its numeric keys. Otherwise, its structure is similar to prior preferred embodiment.

Figure 10 depicts a front side 2 of an electronic card 1. The electronic card 1 has a twelve key keypad 9. Ten of the keys are numeric, for numerals 0-9, and two are special function keys, namely an ENTER key and a CLEAR key. All of the keys are touch activated. In addition, keypad 9 has ten light-emitting diodes ("LEDs"), 101-110, one for each of the numeric keys. It is especially preferred that the LEDs be located in the same corner of each key, but it would also be possible, although less desirable, to make the LEDs a separate element, such as a separate array of LEDs. The electronic card 1 also contains two additional LEDs, 111 and 112, which function as a visual display device for indicating whether a personal identification number ("PIN") has been correctly entered into the card by designating whether the card is ready or whether there has been an error. If desired, the electronic card 1 can also contain one or more special function keys 113.

The purpose of the LEDs 101-110 is to allow a user to confirm correct entry of numbers into keypad 9. After card 1 is turned on by On/Off switch 3, once a numeric key is activated by touch, the LED associated with that LED will light up and remain lit for a specified time or until another key is activated by touch, whichever is shorter. The LEDs can be controlled by an LED driver (not shown). Because there may be times when the user does not want the LEDs to light up, or certain useres who do not want such a feature, the LEDs can be turned off by

entry of a specified preprogrammed code into card 1, and, if subsequently desired, reactivated. Thus, for example, a deactivate or reactivate sequence might be a series of key entries such as ENTER, ENTER, 7, 2, 5, ENTER, ENTER, 7, 2, 5, CLEAR. In addition, in a less desirable alternative embodiment, the LEDs could be deleted in their entirety, or there could be a less than one to one correlation between a key and an LED (for example, there might only be one LED, its only purpose being to confirm activation of any key).

This embodiment does not require any special function keys other than what may exist on keypad 9. By selection of a preprogrammed code into card 1, in the same manner as was just explained, the preprogrammed code can serve the same function as a special function key. For example, such a code might be used to select different uses for the card, such as accessing different accounts. It might also be used to send a special command to the computer to store specified data in a preselected portion of the magnetic storage medium.

Although this preferred embodiment does not require any special function keys other than what exist on keypad 9, it does not preclude their use. If optional special feature keys 113 are included in card 1, they could also trigger or be part of any sequence used to deactivate or reactivate the LEDs or any other function or operation that could be triggered by a special function key. For example, they could be used as a trigger, or be part of a triggering sequence or code, for changing a user identifier stored in the magnetic storage medium affixed to the card that can be read by a standard magnetic stripe reader.

It is also contemplated that this alternate preferred embodiment may require correct entry of a PIN before the card will function, or that a PIN be verified before it is used to generate a user one-time number through use of a card number generator. In either scenario, it is useful for the user to be able to determine whether the PIN has been correctly entered into the card. In either scenario, when the user is ready to enter a PIN into electronic card 1, the user presses the ENTER button. If the correct PIN for the card has been entered, the READY light 111 will light, but if the PIN is incorrect, the ERROR light 112 will light. The CLEAR key clears all entries of earlier information into keypad 9 and allows the user to begin reentering a PIN. If desired, the READY and ERROR

lights can be deactivated or reactivated in the same manner as described for the LEDs.

The versatility of this embodiment will now be illustrated by a theoretical example of how an electronic card in accordance with this embodiment could be used in a number of different situations.

First, assume that the user of the card wants to use the card for a company business expense. In this scenario, the user could select a company credit card, issued in the name of the company, by turning the card on, touching a special function button 113 followed by numeric key 1, then the ENTER key. This could tell the card to use an algorithm for a company account stored in the card's computer. Next, the user would enter the user's PIN for that company account. The card's computer would then generate a payment card number and temporarily store that number, and a user identifier representing the company name, in track 2 of the card's magnetic stripe, which could then be read by a magnetic stripe reader and sent to a verification agency for validation.

Second, assume that the user wants to use the card to charge a personal expense. In this scenario, the user could select a personal credit card by turning the card on, touching a special function button 113 followed by numeric key 2, then the ENTER key. This could tell the card to use an algorithm for a user credit card stored in the card's computer. Next, the user would enter the user's personal PIN. The card's computer would then generate a payment card number and temporarily store that number, and a user identifier representing the user's name (which would be different from the user identifier used in the first scenario), in track 2 of the card's magnetic stripe which could then be read by a magnetic stripe reader and sent to a verification agency for validation. The payment card number generated in this scenario would be different from the payment card number generated in the first scenario in two respects. First, the bank identification number would be different. This is a fixed variable portion of the payment card number (since many different cards for the same bank could have this number). Second, the account number would be different. This is a variable variable portion of the payment card number that changes each time the card is used (this is the same as the individual account portion of traditional credit card numbers).

Third, assume that the user wants to use the card to charge a personal expense, except the user wants to make a note that the expense is tax deductible. This scenario would proceed the same as the second scenario, except that a second personal PIN would be entered. In this example, the fixed variable portion of the payment card number would be the same as in the second scenario, but the variable variable portion would be different.

Fourth, assume that the user now wants to use the card to enter a parking garage controlled by an access card, and the requisite code has been stored in the card's memory. In this scenario, the user could access the requisite code by turning the card on, touching a special function button 113 followed by numeric keys 98, then the ENTER key. This could tell the card to temporarily store the requisite code in the card's magnetic stripe, which could then be read by a magnetic stripe reader.

Fifth, assume that the user now wants to use the card to enter the building of the parking garage, and this requires a PIN plus the requisite code of the fourth scenario. This would proceed the same as the fourth scenario, except that the user would enter the PIN into the card and it would be added to the magnetic stripe with the requisite code.

As should be apparent from these limited examples, there are many ways that an electronic card according to the present invention can be used.

3. A method for transferring a data packet from a user of an electronic card to a money source as part of a payment card transaction

The electronic cards of the preferred embodiments can be used to allow a standard magnetic stripe reader to read a data packet that is submitted to a money source for approval of a given payment card transaction associated with the data packet.

When such a data packet is read and transmitted to a money source, additional information can be conveyed within the data packet, as long as it can be conveniently read by the money source. This is why it is especially preferred that the data packet be encoded in the second track of the magnetic stripe within the field of data that can be read in a normal credit card transaction. Combination of this capacity for transmission of data with the flexibility provided by use of the

encoding technology opens a communication channel for data transmission that can be exploited every time such a transaction takes place.

One way to exploit the communication channel is to use it to directly convey information from the electronic card to the money source. This can be useful in synchronizing the electronic card with the money source. For example, it can be used to provide the money source with a current sequence number of the electronic card used in generating a one-time unique purchase order number. (The sequence number can be used in connection with an algorithm that is executed that uses the selected user key and a customer sequence number to generate the Coupon. The sequence number is changed after each Coupon is generated and a new Coupon can then be generated using the changed sequence number and a selected user key for the new Coupon.) It can also be useful in providing the money source with results of diagnostic test programs that are periodically run by the electronic card's computer, an important example of which is remaining battery capacity

Because of the limited capacity of current batteries that are useful in the type of electronic card described herein, it is possible that the battery will cease working before an expiration date of the card if the electronic card is heavily used. To solve this problem, the computer can run a program that measures remaining battery capacity or checks for a battery life parameter and generates a warning signal when a low battery condition is detected. The computer could even run a predictive program estimating when the useful battery capacity will expire based upon past usage, and this program could generate a battery life signal related to an estimated remaining battery life of the battery, which could be sent to the money source. The money source, in turn, can use such diagnostic information to send out a new electronic card to the user before the electronic card runs out of battery life. The same type of communication system can be used for other diagnostic programs that measure at least one parameter and generate a warning signal when a preselected threshold is exceeded.

Another way to exploit the communication channel is to use it to directly convey information that is generated by a user of the card to the money source. For example, the user could include a customization variable in the data packet.

4. A method for customizing use of an electronic card through a customization variable

Like a traditional payment card number, a one-time payment card number should be capable of being read by a standard magnetic stripe reader when it is part of a physical card used in traditional face-to-face transactions in which a user presents the physical card to a merchant for payment. However, like traditional payment card numbers, a one-time payment card number should also be capable of being used in a Mail Order Telephone Order ("MOTO") credit card transaction between the user and a merchant. Thus, like a traditional payment card number, the one-time payment card number should fit within, and work with, present platforms and protocols for financial transactions involving payment cards, such as traditional credit cards. This versatility allows the one-time payment card number to be used with electronic cards, software programs used in network applications, or telephones (especially telephones used in what is now being referred to as m-commerce, or mobile commerce).

A traditional payment card number can be characterized as having three parts. First, there is a set of fixed variables. This contains numerals that represent certain specified data fields, such as a bank identifier and a month and year expiration date for a given payment card. (The "bank" may be any "money source" as that term has been defined in U.S. Patent No. 5,937,394.) Second, there is a set of variable variables. This contains numerals that will vary for different payment cards issued by the same money source. In other words, this is the portion of the card number that will be specific to an individual entity or account for a given issuing money source. Third, there is a check sum digit. The value of the check sum digit is dictated by the other numerals in the card number.

In the context of the present invention, a user one-time payment card number is akin to a traditional payment card number, with certain exceptions. In a traditional payment card number, there might be a set of six fixed variables, followed by a set of nine variable variables, followed by a check sum digit and another set of four fixed variables representing the month and year. When a user uses this traditional payment card number to complete a given financial transaction, the transaction is always completed by using the same twenty digits for the payment card number. By contrast, if the user uses a one-time payment

card number to complete any such given financial transaction, the transaction will not be completed by always using the same twenty digits for the payment card number. Instead, the twenty digits of the one-time payment card number will vary, and the degree to which they vary may depend upon user selection of a customization parameter. In addition, because the one-time payment card number varies with successive usage, the check sum digit will not necessarily be the same with successive usage, although it may be. Thus, the check sum digit must be recalculated for each new one-time payment card number, and this is why it shall be referred to as a "check sum variable" in the context of a one-time payment card number according to the present invention.

Another difference between a traditional payment card number and a one-time payment card number is the way that a given transaction using either number is validated by a verification agency, which may be a money source or an entity who processes payment card transactions. When a transaction involving a one-time payment card number is processed, the verification agency must verify that the one-time payment card number is valid for the user identifier for the particular given transaction, as opposed to any given transaction involving the user identifier. (The verification process must take into account how selection of the customization parameter may affect what the verification agency will receive for verification.) This difference is a reason why use of the one-time payment card number provides greater security and anonymity than can be obtained through use of a traditional payment card.

A card number generator generates a one-time payment card number. No matter what method is used to generate a one-time payment card number, two successive one-time payment card numbers should be different. This can be accomplished by using a sequence number that is changed after each one-time payment card number is generated. (The present invention does not require that all theoretical possibilities will result in different one-time payment card numbers. Instead, it is preferred that there be a low probability of occurrence of identical one-time payment card numbers attributable to convergence of two different inputs leading to the same result due to operations performed on the inputs by the algorithm.)

A user can customize use of an electronic card having a card number that varies with each use by selecting at least one customization parameter to customize a given use of the electronic card. There are three general customization parameters that can be used to customize a given use.

First, the user can customize generation of the one-time card number. This can be done many different ways. An example of one way in which it can be done is to customize selection of a selected user key that is used to generate the one-time card number. Another way in which it can be done is to include a customization variable in the one-time card number, or as an input into the algorithm used to generate the one-time card number.

Second, the user can customize the user identifier that is used to validate the one-time card number. This can be done many different ways. One way is to choose one of two or more preselected identifiers as a selected user identifier. Another way is to modify the user identifier. Still another way is to add a customization variable, such as a numeric character, to the user identifier at a preselected location.

Third, the user can include a customization variable with information transmitted to a verification agency for validation of the given use. Unlike the first two customization parameters, this parameter relies upon use of an additional field of data collected as part of the validation process for a given transaction, and this may require a change in established validation protocols. It is especially preferred that any such change be technically feasible within the confines of hardware that is being used to process traditional payment card transactions. In the context of an electronic card with a magnetic stripe, this means that it is preferred that the additional customization variable be stored in the magnetic stripe, and it is especially preferred that it be stored in the second track of the magnetic stripe.

Once it is recognized that using one or more of the foregoing customization parameters will customize a given transaction involving use of a one-time payment card number, and that such customization will seamlessly allow a user to transmit additional information to the money source processing such transaction, without loss of desired security or anonymity, the options for using such customization are virtually limitless.

After a one-time payment card number is validated for a given transaction, the money source can determine what customization parameter(s) was selected by the user for the given transaction, which allows the money source to determine what handling option should be used for the transaction involving the one-time payment card number. (It also allows the money source to determine what sequence number is associated with the one-time payment card number, so that its records can be synchronized as part of the validation process.)

One use of multiple handling options is to allow the money source to access multiple accounts. For example, a user might use one account as a credit card, and another account as a debit or checking card. By choosing which account should be used for a given transaction, the user could determine, at the point of use, whether to charge the transaction, or have it deducted from an existing account balance. The same idea could be used for multiple credit cards, whether they are from the same issuer or different issuers, or even different cards, such as Visa®, MasterCard®, Diner's Card®, Discover® or American Express®. In addition, the user might elect to have separate billing statements for separate accounts, or have all billing consolidated in a single statement.

Another use of multiple handling options is to allow identification of the person completing a transaction, or to allow multiple persons access to a single account, or place different restrictions on multiple persons on a single account. For example, a single account might be opened with an issuing bank, but an entire family might be authorized to use the account. Thus, a father and a mother might have their own customization parameter, a teenage child might have another customization parameter and a lower authorized spending limit, and a preteen child might have a fourth customization parameter, but only be authorized to engage in a certain limited number of transactions per time period with a maximum spending limit for each transaction. All the members of this family could use the same card number generator embedded within a PDA or mobile phone, or on a computer or in an electronic card. At the end of a specified billing cycle, all transactions completed by any member of this family could be consolidated in a single bill, and that bill could indicate who spent what when during the billing cycle, and what it was spent on.

Still another use of multiple handling options is to allow a user to classify the nature of a particular transaction at the time it is completed. For example, suppose an individual uses a single credit card for personal expenditures and business expenditures. By assigning one customization parameter to personal transactions, and a second customization parameter to business transactions, the user can simplify accounting for such transactions without the necessity of having and carrying two separate cards. If desired, the user could even receive two separate statements for such expenditures so that the personal expenditures would not be discernable from the documentation associated with the business expenditures. Individual transactions could also be classified according to a preselected set of criteria, and such criteria could be used in various financial programs. For example, a user might include a code classification system used in a money management system to create various reports that itemize categories of spending or assist in budgeting of finances.

Yet another use of multiple handling options is to allow a user to preselect how a particular transaction is treated in a subsequent bill. For example, an individual user might not want a billing statement to include information about the identity of second entities who provide certain goods or services, or when transactions with such entities take place, but still want to have the billing statement include such information for other transactions. By selecting two different customization parameters with these two different handling options, the user has the option of controlling what information it receives in billing statements about individual transactions.

Multiple handling options can also be used to guard privacy, or for commercial purposes that do not presently exist. For example, the user and the money source might enter into an agreement about how, and under what circumstances, the money source can distribute information about transactions of the user, depending upon which customization parameter is used in a given transaction. The agreement might provide different levels of confidentiality, and set up different levels or types of compensation tied to transactions falling within the different levels for a given time period.

One level of confidentiality might restrict distribution of any information concerning a transaction by the money source to any third party. For example, a

user might want strict confidentiality of any transaction involving medical services, and would not want the money source to divulge that information to any party unless legally required to do so. Or, maybe the user does not want any third party to learn of any transaction that exceeds a certain dollar amount, for fear of a potential deluge of unsolicited advertising. A user might pay a monthly fee for use of this option, a transaction based fee, or no fee at all.

A second level of confidentiality might permit distribution of any information concerning a transaction by the money source to any third party. Such information is potentially valuable for purposes of advertising, and creating profiles for targeted marketing, and the money source might even pay the user for the right to sell such information.

Other levels of confidentiality might fall between those already noted. For example, a third level might permit distribution of certain information concerning a transaction (such as the payee, the amount of purchase, the date of purchase, and a profile of the user), but restrict distribution of other information concerning a transaction (such as the identity of the user). Another level of confidentiality might restrict distribution of information concerning a transaction to any third party, but allow the money source to use such information for its own marketing efforts directed to the user.

5. Anonymous delivery system

By using a customization parameter, use of a one-time payment card number can be customized for a desired delivery method, as will now be explained.

When a user purchases certain goods or services, the delivery or availability of such goods or services can be immediate and made at the time and point of purchase, and therefore can be anonymous. Examples of this include use of a payment card in a face-to-face transaction at a check out counter or use of a payment card to obtain immediate access to something, such as a service, information or a software program, that is delivered telephonically or over a computer network. In such situations, the user may not be required to provide the merchant with a user address. However, even if an address is required, it need not be used for delivery, so it need not be an actual address of the user or an

address for delivery of goods. Accordingly, in such situations, the user might want to provide a meaningless address to avoid undesired solicitation and junk mail, or an address of somebody who screens anything received at the address. Such an address could be a Proxy Agent.

When a user purchases goods that have to be delivered, the user is traditionally faced with a dilemma. Before the goods can be delivered, the user has to provide an address for delivery. If a home address is used, so the goods can be conveniently delivered to the home, anonymity is sacrificed. Once a merchant or marketer has a home address, the address is available for solicitation and, unfortunately for many consumers, junk mail. In addition, once a merchant or marketeer has a home address, it can be cross-referenced against available data bases, which can often reveal the true identity of the user, even if the transaction was otherwise conducted anonymously through use of a one-time payment card number and a fictitious user name. Once a true identity is obtained, that identity can be matched with the purchase, and this information can be used for all sorts of marketing purposes, including telemarketing. As is readily apparent, use of a real home address, even with an otherwise anonymous payment transaction, can lead to significant loss of a user's privacy and unwanted intrusions upon such privacy by a variety of marketing methods and practices.

To avoid such loss of privacy, a user might request that the goods be delivered to an address other than the user's home address, such as a work address or an address used for delivery of mail, such as a post office box. However, this option eliminates the convenience of a home delivery, and creates additional inconvenience. It is also not an option if the user making the purchase wants the goods sent to a third party, such as a relative, for a birthday or a holiday gift. This problem is aggravated when the desired delivery date is crucial and there is not sufficient time for delivery to a secondary address, and then a second delivery to the intended recipient. (In addition, this would involve extra cost and inconvenience associated with receiving the shipment at the secondary address, and then resending the package to the desired recipient.)

Even when a user is willing and able to put up with the inconvenience of delivery to a secondary address, there may be additional drawbacks with such a delivery.

The user may not want some goods delivered to the user's work address for a variety of reasons, including a resultant loss of privacy associated with such delivery. Not only may the user want to prevent colleagues from knowing what the user has purchased, but delivery to a work address may lead to junk mail being sent to the work address, or correlating the work address, in one fashion or another, to the true identity of the user. For example, assume that the user uses a fictitious name and a work address. The delivery agent may require proof that the user is entitled to receive the goods, and this proof could compromise the user's true identity. Alternatively, the user might not be able to claim goods delivered to the user's work address, or such goods, even if they have been delivered to the work address, may not reach the user due, for example, to theft by another employee.

Although delivery to an address designated for pick-up may avoid some of the problems associated with delivery to a work address, it has other drawbacks. For example, it requires that the user have an account with the delivery address, and pay for this service. In addition, it does not prevent the address from being used for junk mail. And, unless the user is careful with use of the address, and the service guarantees anonymity, it might still be possible for marketeers to use a database to cross-reference the delivery address to develop the true identity or address of the user.

To avoid the foregoing problems, the preferred embodiment of the present invention allows a user to select an anonymous delivery option when a one-time card number is used with a user identifier to complete a given commercial transaction. The mechanics of the anonymous delivery option can be triggered by use of a customization parameter associated with the anonymous delivery option. By selection of an appropriate customization parameter, a user can select from a variety of different, anonymous delivery options. For example, one option might be home delivery. Another option might be a pick-up by the user at a specified address. Another option might be a handling option by which the user selects a preselected delivery address. Still another option might be an alternative handling option by which the user provides a specified one-time delivery address for the specific transaction, and this might be provided before or after the actual transaction is completed with a merchant.

Once the anonymous delivery option is triggered, it can be implemented as follows.

When the commercial transaction is completed, whether it is a face-to-face transaction or a MOTO transaction, the user will provide the merchant with a one-time payment card number and a user identifier. As already noted, the user can customize the one-time payment card number so as to select the desired delivery method and address. Or, alternatively, the merchant could specify who the delivery agent will be, such as Federal Express® or UPS®, and the user could still specify a delivery option for such a carrier by selection of an appropriate customization variable. Once the merchant receives this information, it is sent to a money source to confirm the validity of the transaction. The communication from the merchant to the money source will also include an identification of the merchant and the amount of the transaction, and will also typically include the date of the transaction. When the money source confirms the validity of the transaction, the money source will send the merchant a confirmation number that can be used to identify the transaction. In other words, so far, this transaction proceeds in the same fashion as an ordinary credit card transaction, except that the merchant does not yet have a delivery address for the goods.

The delivery address can be provided to the delivery agent in a number of ways without allowing the merchant to learn the delivery address.

One way the delivery address can be kept from the merchant is for the money source to provide the delivery address to the delivery agent along with a tracking identifier. The money source can also give the tracking identifier to the merchant, so that it can serve as an identifier for the shipping process. The tracking identifier might simply be the confirmation number that the money source gave the merchant to confirm validation of the commercial transaction, or it might be another number specifically designated for this purpose. Once the merchant has the tracking identifier, the goods can be delivered to the delivery agent with the tracking identifier taking the place of a delivery address.

After the delivery agent receives the goods, the tracking identifier can be used to access the delivery address. Now the delivery agent to the delivery address can deliver the goods, and the delivery agent need not have any information about the addressee. To confirm delivery, and to verify that delivery

has been made to the right party, the delivery agent can be given a delivery code. This might be information about the commercial transaction, such as a merchant invoice number or the one-time payment card number used to complete the transaction, but it is preferably a separate code that the merchant, and the merchant's employees, would not have access to. The delivery code can be generated by the delivery agent or the money source, or even the user, as long as it is known by the delivery agent and the person who will pick up the goods, who will be designated the "addressee" (the addressee may be the user or a third party). By using the money source or another source as an intermediary, there need not be any direct contact between the delivery agent and the addressee until the time of delivery.

Another way the delivery address can be kept from the merchant is to use two delivery agents, or to deliver the goods to a destination address where the purchased item is held at a pick-up location for pick-up by the addressee. For example, the goods could be delivered to a local office of the delivery agent. In both of these cases, the first delivery agent will not have an address of the addressee, and the merchant could not get such an address from the first delivery agent. A variant on this method of delivery is to segregate knowledge of the delivery address within the delivery agent. For example, the delivery agent might use an internal delivery address for the first point of delivery. This might be a central location where a number of packages from a given collection zone are collected for sorting and subsequent distribution. Once the goods reach this central address, they could be processed according to special procedures to limit access to the correlation between the tracking identifier and the delivery address.

If the goods are not to be shipped by use of a delivery agent, but held for pick-up by the user or an authorized agent of the user, the delivery process can be modified in a number of ways to safeguard anonymity, while still providing security against fraud. For example, the money source can send a delivery code to the user and the merchant that the user must have at the time of pick-up. The user can also be required to provide an additional verification of identity, albeit anonymous to the merchant, at the time of pick-up. One way to do this is to require the user to provide a valid one-time payment card number at the time of pick-up, and it is especially preferred that this number be a dummy number that is

designated as such by using a customization variable designated as a dummy variable. When the dummy one-time payment card number is submitted for verification, the dummy variable tells the money source that this is not a commercial transaction, but rather, a request for verification of valid identity, and that it should be treated as such. Thus, the money source can use the dummy one-time payment card number to confirm that the person picking up the goods is authorized to pick them up, and then send a confirmation of the transaction to the merchant to verify that the party presenting the dummy one-time payment card number should be allowed to pick-up the goods. This confirmation also creates a record of receipt of the goods by the user. And, of course, all of these same methods could also be applied, if desired, to the situation of a delivery by the delivery agent to a delivery address.

In an alternative embodiment, the methods for anonymous delivery can be used to implement an anonymous "charge on delivery" that is somewhat akin to the concept of cash on delivery. In this embodiment, the money source can put a hold on charging or debiting the user's account (and, if desired, paying the merchant), until there has been an actual delivery of the goods. One way to establish such delivery is through use of a "dummy" one-time payment card number.

As described above, at least four parties are involved in completing an anonymous delivery of goods when the user does not pick up the goods from the merchant. In an alternative embodiment of the present invention, a fifth party is deliberately placed into the loop as an intermediary to act as a further safeguard against loss of anonymity. The fifth party, which shall be referred to as "Privacy Systems," can function as a further buffer and safeguard of the user's privacy. Using Privacy Systems as a payor to the merchant, a payee to the money source and the clearinghouse for all of the details of a given transaction, including the delivery address, does this. By adding this fifth party, who might be legally obligated not to divulge preselected details of a given transaction to third parties without consent of the user, the money source is taken out of the loop as a coordinating party with knowledge of all of the transaction details. Privacy Systems can also function as a clearinghouse for collecting, categorizing,

marketing and selling information about transactions in which it is serving as an intermediary.

Although the foregoing detailed description is illustrative of preferred embodiments of the present invention, it is to be understood that additional embodiments thereof will be obvious to those skilled in the art.

Accordingly, it will be readily apparent to those skilled in the art that still further changes and modifications in the actual concepts described herein can readily be made without departing from the spirit and scope of the disclosed inventions as defined by the following claims.

What is claimed is:

1. A method for transferring a data packet from a user of an electronic card to a money source as part of a payment card transaction, comprising the steps of:

executing a program on a computer of the electronic card to generate a data packet that can be read by a standard magnetic stripe reader;

using the standard magnetic stripe reader to read a payment card number, a user identifier and the data packet as part of a given payment card transaction; and

submitting the payment card number, the user identifier and the data packet to the money source for approval of the given payment card transaction.

2. A method as recited in claim 1, wherein the program is a diagnostic program that measures at least one parameter and generates a warning signal when a preselected threshold is exceeded.

3. A method as recited in claim 2, wherein the program checks for a battery life parameter and generates a warning signal when a low battery condition is detected.

4. A method as recited in claim 1, comprising the further steps of:

generating a user one-time payment card number through use of a card number generator; and

using the user one-time payment card number as the payment card number.

5. A method as recited in claim 4, wherein the one-time payment card number is correlated with a sequence number that indicates the relationship of the one-time payment card number to a sequence of one-time payment card numbers generated by the card number generator.

6. A method as recited in claim 5, wherein the data packet can be used to obtain the user sequence number.

7. A method for alerting a money source to a low battery condition of a battery used in an electronic card, comprising the steps of:

(1) using the electronic card to conduct a plurality of payment card transactions in which a payment card number and a user identifier are submitted to the money source as part of an approval process;

(2) executing a program on a computer of the electronic card to check for a battery life parameter and generate a warning signal when a low battery condition is detected; and

(3) when a warning signal is generated, submitting a low battery indicator to the money source in connection with the approval process.

8. A method as recited in claim 7, wherein the program is executed each time the electronic card seeks approval of a preselected number of payment card transactions.

9. A method as recited in claim 8, wherein the program generates a battery life signal related to an estimated remaining battery life of the battery.

10. A method as recited in claim 9, comprising the further step of:

(4) submitting a battery life indicator that is based upon the battery life signal to the money source in connection with the approval process.

11. A method as recited in recited in claim 10, comprising the further step of:

(4) providing a user of the electronic card with a replacement electronic card before the battery life parameter drops below a selected threshold.

12. A method for allowing customized use of an electronic card having a card number that varies with each use, comprising the steps of:

(1) allowing a user to select a customization parameter to customize a given use of the electronic card by at least one of the following steps:

(a) customizing generation of a one-time card number;

(b) customizing a user identifier; or

(c) inclusion of a customization variable with information transmitted to a verification agency for validation of the given use;

(2) generating a user one-time payment card number through use of a card number generator;

(3) submitting the user one-time payment card number and the user identifier to a verification agency for validation, and, if the user has selected step (1)(c), including the customization variable with the submission for the given use; and

(4) verifying that the one-time payment card number is valid for the given use.

13. A method as recited in claim 12, wherein the electronic card is a payment card and the one-time card number is a one-time payment card number.

14. A method as recited in claim 13, wherein the card number generator generates a new card number by executing an algorithm that uses a selected user key to generate the new card number.

15. A method as recited in claim 13, wherein the user can customize generation of the one-time card number by choosing either a first user key or a second user key as the selected user key, and wherein the algorithm will generate a first one-time card number if the selected user key is the first user key or a second one-time card number if the selected user key is the second user key, the first and the second one-time card numbers being different, but both valid with the user identifier.

16. A method as recited in claim 12, wherein the electronic card is comprised of:

a card base;

a computer affixed to the card;

an input mechanism;

a magnetic storage medium affixed to the card that can be read by a standard magnetic stripe reader;

an encoder for generating a data packet that is stored in a designated portion of the magnetic storage medium and is readable by a standard magnetic stripe reader; and

a power source for supplying power to the computer and the encoder;

wherein the electronic card is sized such that the magnetic storage medium can be read by the standard magnetic stripe reader.

17. A method as recited in claim 16, wherein the data packet is further comprised of the customization variable.

18. A method for processing a plurality of payment card transactions based upon a user's selection of a customization variable for each of the transactions, comprising the steps of:

(1) establishing a plurality of handling options between a money source and the user;

(2) providing the user with a card number generator;

(3) allowing the user to complete a plurality of payment card transactions within a time period in accordance with the following steps:

(a) allowing the user to select a customization parameter to customize a given use of the card number generator by at least one of the following steps:

(i) customizing generation of a one-time payment card number;

(ii) customizing a user identifier; or

(iii) inclusion of a customization variable with information transmitted to a verification agency for validation of the given use;

(b) generating a user one-time payment card number through use of the card number generator;

(c) verifying the validity of the given use by submitting the user one-time payment card number and the user identifier to a verification agency for validation, and, if the user has selected step (3)(a)(iii), including the customization variable with the submission; and

(d) repeating steps (a) through (c) at least once within the time period; and

(4) processing each of the plurality of payment card transactions in accordance with one of the plurality of handling options based upon the customization parameter selected for each of the plurality of payment card transactions.

19. A method as recited in claim 18, wherein the card number generator is included within an electronic payment card.

20. A method as recited in claim 19, wherein the electronic payment card is comprised of:

a card base;

a computer affixed to the card;

a keypad for providing input to the computer, the keypad having ten numeric keys and at least one special function key that are touch-activated;

a magnetic storage medium affixed to the card that can be read by a standard magnetic stripe reader;

an encoder controlled by the computer for generating a data packet that is stored in a designated portion of the magnetic storage medium; and

a power source for supplying power to the computer and the encoder;

wherein the electronic card is sized such that the magnetic storage medium can be read by a standard magnetic stripe reader.

21. A method as recited in claim 18, wherein the first and the second handling options are mechanisms to bill two separate accounts.

22. A method as recited in claim 19, wherein the user is sent a single bill for charges to the two separate accounts.

23. A method as recited in claim 22, wherein the user is sent a first bill for the first account and a separate bill for the second account.

24. A method as recited in claim 18, wherein the first and the second handling options are a first and a second mechanism for dealing with distribution of information concerning the plurality of payment card transactions.

25. A method as recited in claim 24, wherein the first mechanism restricts the distribution from the money source to a third party of information relating to any payment card transaction in which the user payment card number was generated by use of the first user key.

26. A method as recited in claim 24, wherein the first mechanism restricts the distribution from the money source to the second entity of personal information of the user relating to any payment card transaction in which the user payment card number was generated by use of the first user key.

27. A method as recited in claim 25, wherein the user provides the money source with consideration for use of the first mechanism.

28. A method as recited in claim 24, wherein the second mechanism permits the distribution from the money source to a third party of information relating to any payment card transaction in which the user payment card number was generated by use of the second user key.

29. A method as recited in claim 28, wherein the second mechanism permits the distribution from the money source to the second entity of personal information of the user relating to any payment card transaction in which the user payment card number was generated by use of the second user key.

30. A method as recited in claim 28, wherein the money source provides the user with consideration for use of the second mechanism.

31. A method as recited in claim 18, wherein the first and the second handling options provide a mechanism for classifying the nature of the plurality of payment card transactions.

32. A method as recited in claim 31, wherein the first handling option is used for business transactions and the second handling option is used for personal transactions.

33. A method as recited in claim 18, wherein the first and the second handling options provide a mechanism for identifying either a first user or a second user as the user.

34. A method as recited in claim 33, wherein approval of a payment card transaction for the first user is subject to different restrictions than approval of a payment card transaction for the second user.

35. A method as recited in claim 18, wherein the first and the second handling options provide a mechanism for controlling what information is reported about the plurality of payment card transactions in a billing statement.

36. An electronic card, comprising:

a card base;

a computer affixed to the card;

a display mechanism controlled by the computer;

an input mechanism;

a magnetic storage medium affixed to the card that can be read by a standard magnetic stripe reader;

an encoder for generating a data packet that is stored in a designated portion of the magnetic storage medium; and

a power source for supplying power to the computer and the encoder;

wherein the electronic card is sized such that the magnetic storage medium can be read by a standard magnetic stripe reader.

37. An electronic card as recited in claim 36, wherein the magnetic storage medium is a magnetic stripe.

38. A method for providing a secure and anonymous transaction between a user and a merchant with subsequent delivery of a purchased item, comprising the steps of:

(1) establishing a user account between a money source and the user which is associated with a fictitious user identifier, a user account number, and a user settlement mechanism through which the user and the money source can settle payment card transactions involving the user account;

(2) providing the user with a card number generator;

(3) completing a payment card transaction between the user and the merchant in which the user account is charged a monetary value for the purchased item, comprising the following steps:

(a) allowing the user to select a customization parameter associated with an anonymous delivery option for subsequent delivery of the purchased item to customize the payment card transaction by at least one of the following steps:

(i) customizing generation of a user one-time payment card number;

(ii) customizing the user identifier; or

(iii) inclusion of a customization variable in a user transaction data packet that includes the user one-time payment card number and the user identifier;

(b) generating the user one-time payment card number through use of the card number generator; and

(c) providing the merchant with the user transaction data packet;

(4) submitting a merchant transaction data packet to the money source, wherein the merchant transaction data packet includes the user transaction data packet, the monetary value, a merchant identifier and a purchased item identifier;

(5) providing the merchant with a confirmation that the transaction is valid after the money source verifies that the user one-time payment card number is valid for the user identifier and the transaction;

(6) sending a tracking identifier from the money source to the merchant;

(7) sending the tracking identifier and a delivery address from the money source to a delivery agent;

(8) invoking the settlement mechanism to charge or debit the user account for a transaction amount correlated to the monetary value;

(9) delivering the purchased item to the delivery agent with the tracking identifier; and

(10) delivering the purchased item from the delivery agent to the delivery address.

39. A method as recited in claim 38, wherein the merchant is not provided with the delivery address.

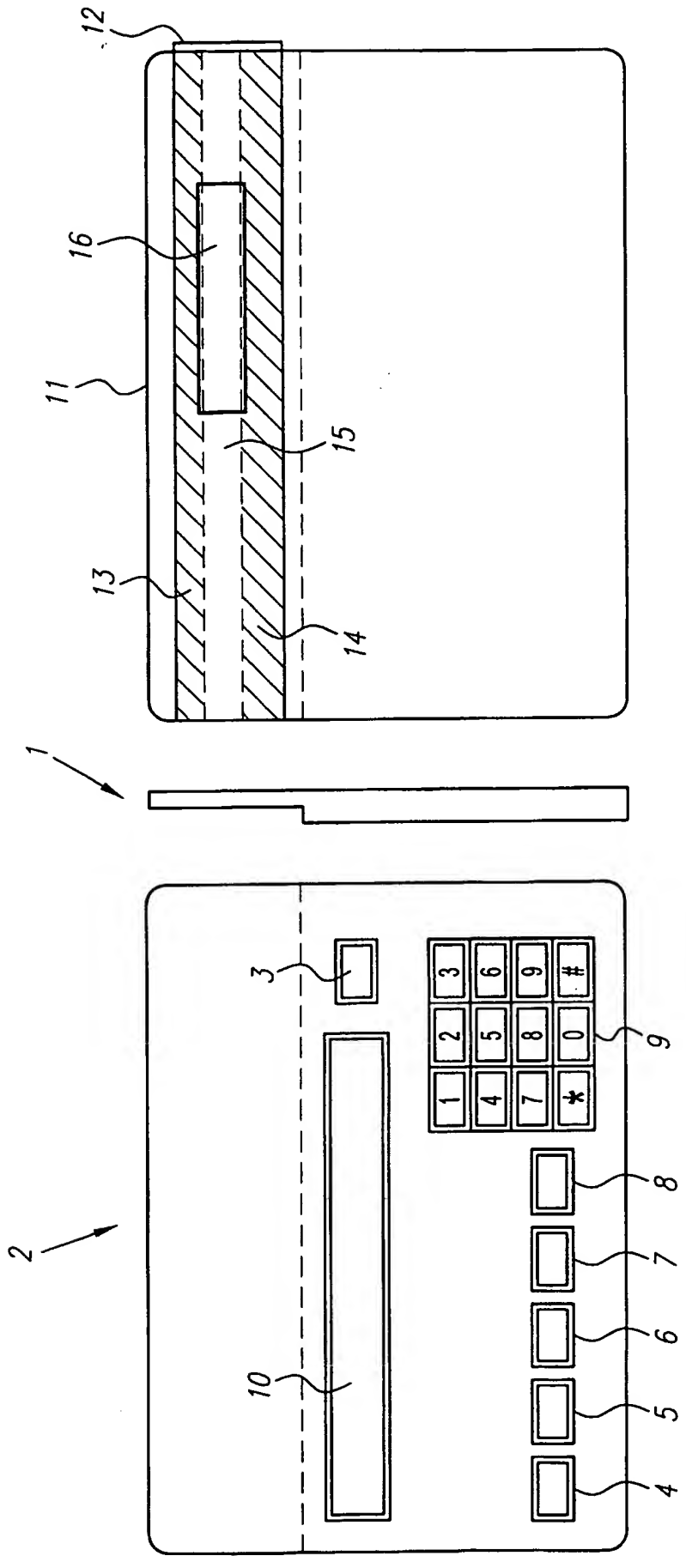


FIG. 1C

FIG. 1B

FIG. 1A

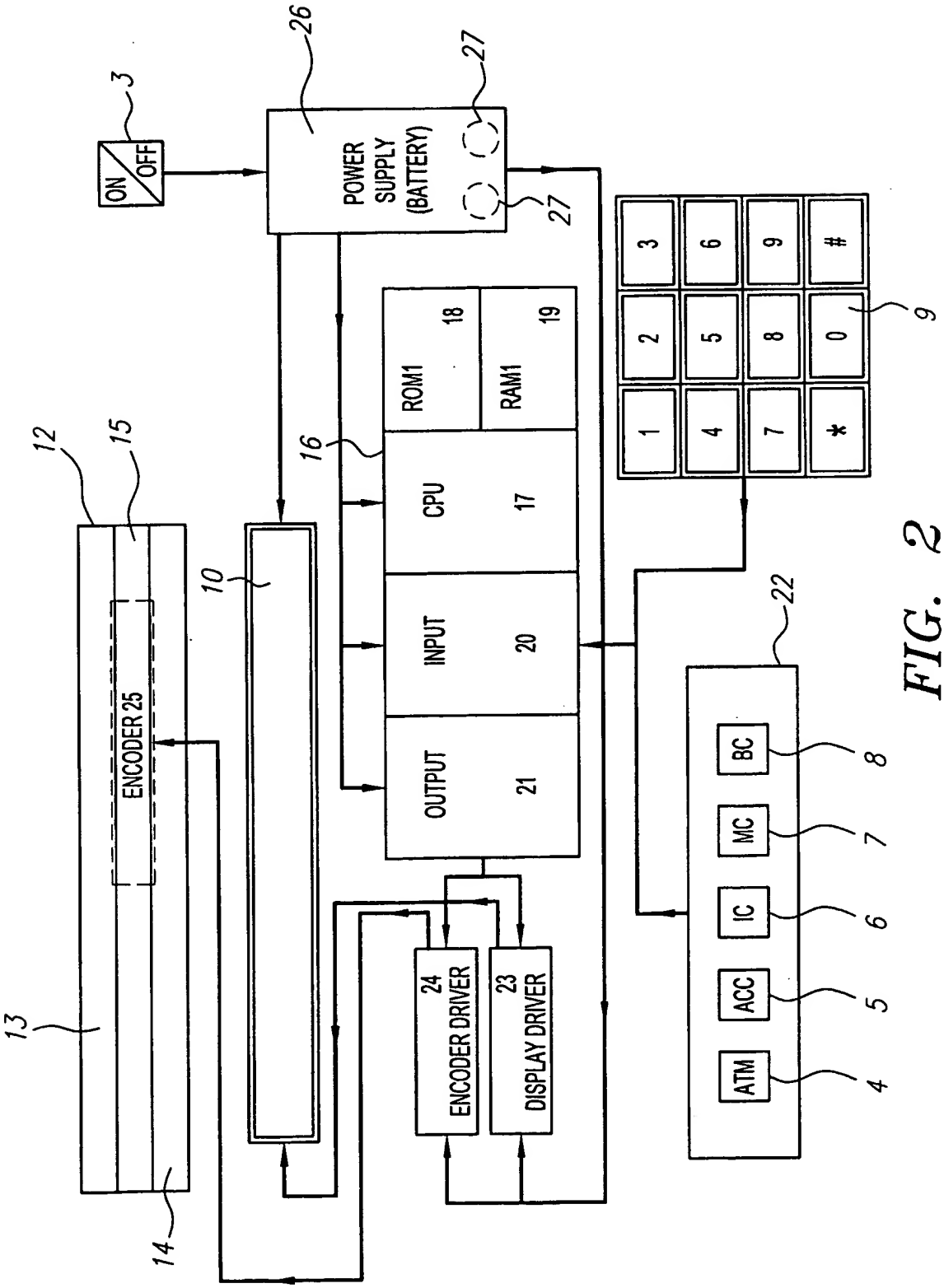

3
ON
OFF
26
POWER SUPPLY (BATTERY)
27
27
ROM1
18
RAM1
19
CPU
17
INPUT
20
OUTPUT
21
16
3
6
9
#
2
5
8
0
9
1
4
7
*
12
15
ENCODER 25
10
22
BC
8
MC
7
IC
6
ACC
5
ATM
4
24
ENCODER DRIVER
23
DISPLAY DRIVER
13
14

FIG. 2

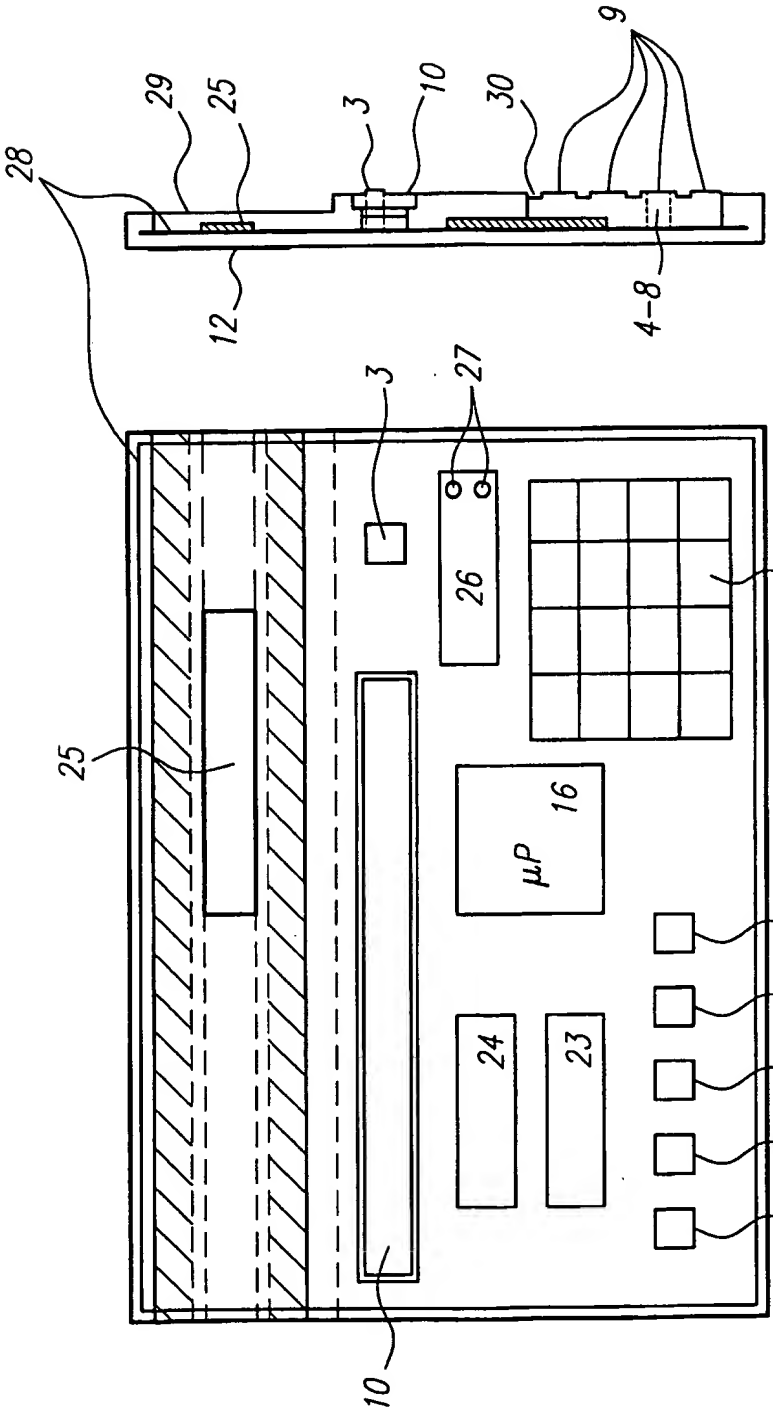


FIG. 3B

FIG. 3A

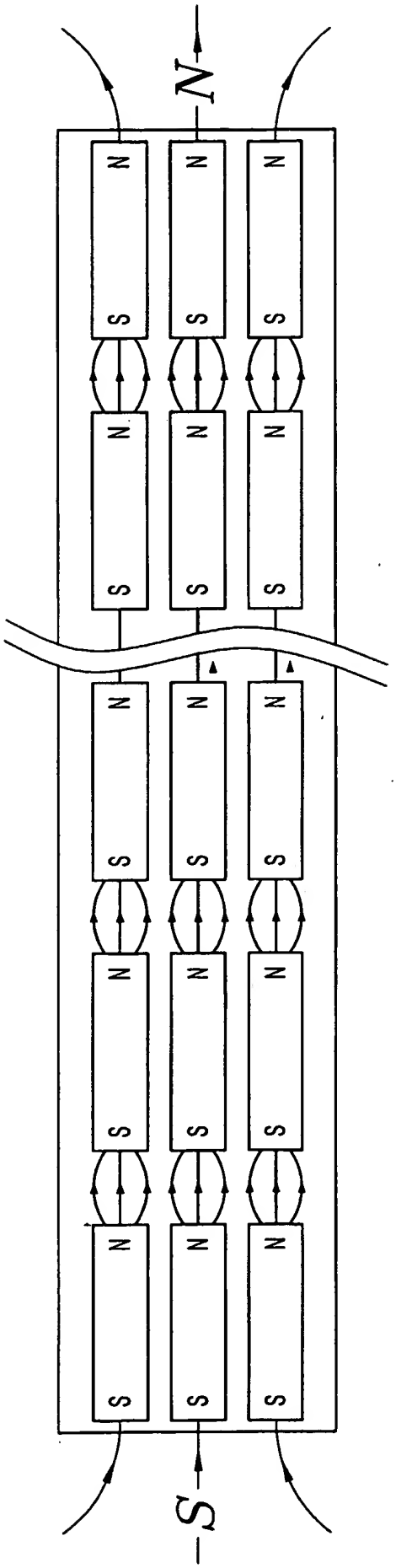


FIG. 4

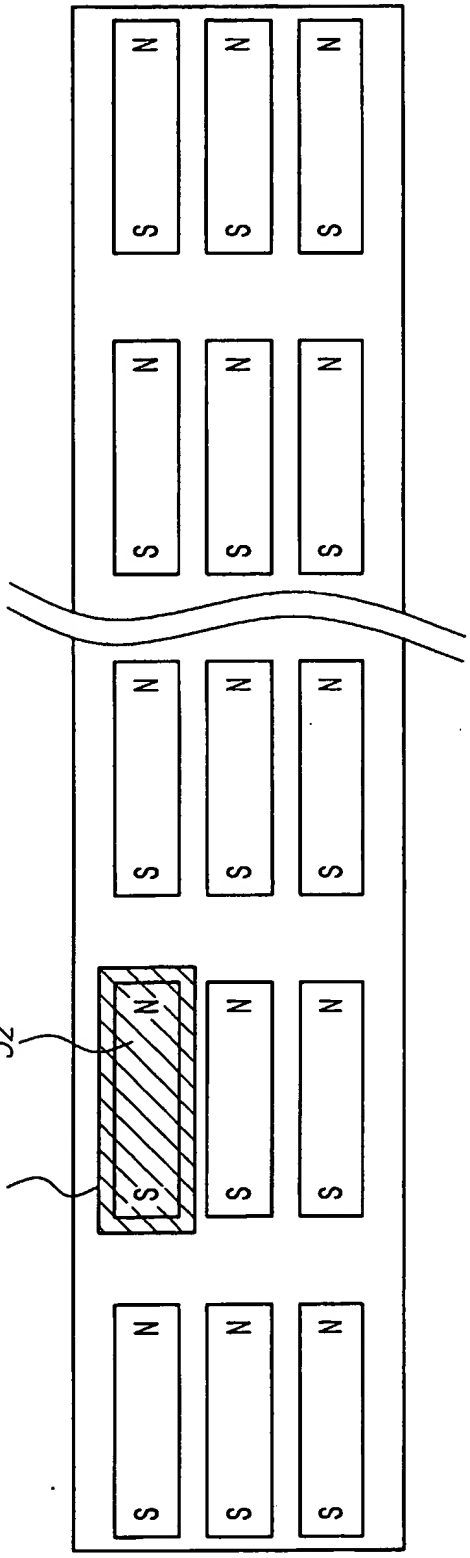


FIG. 5

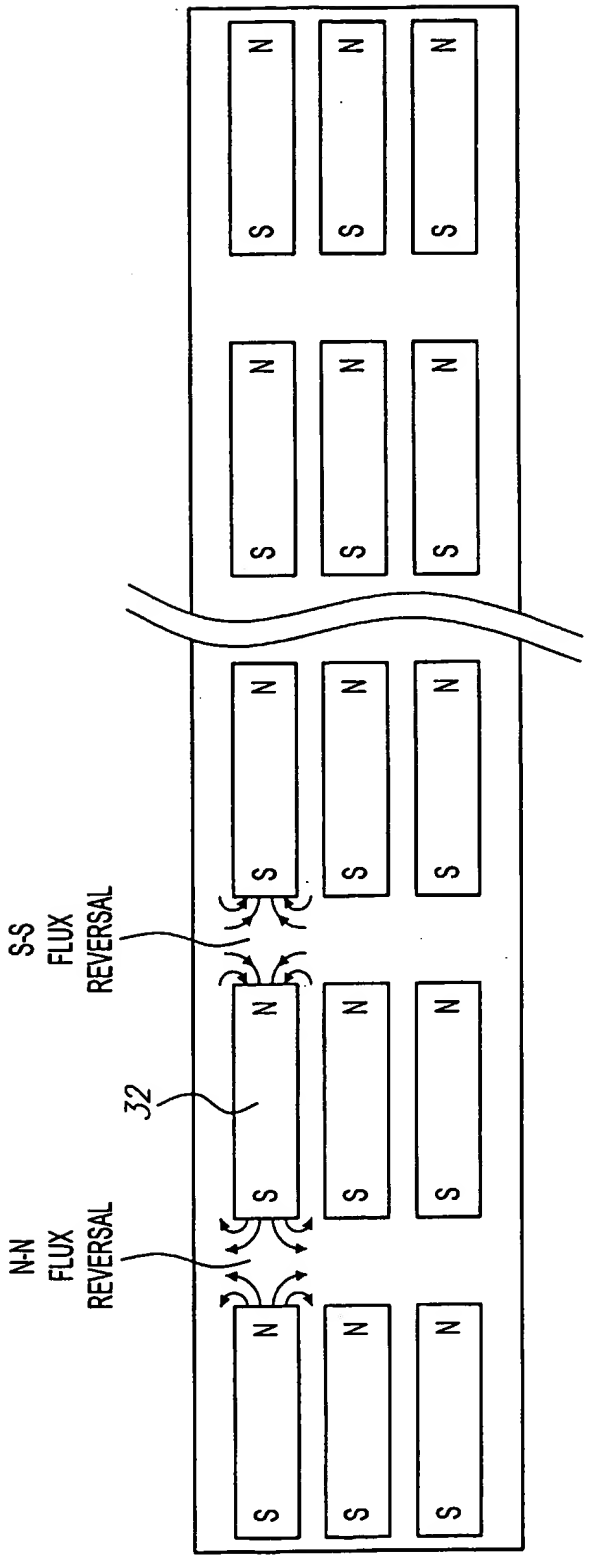


FIG. 6

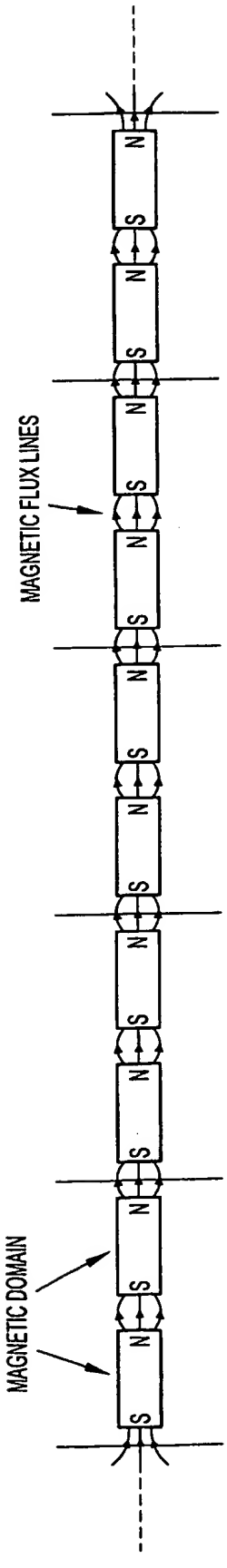


FIG. 7A

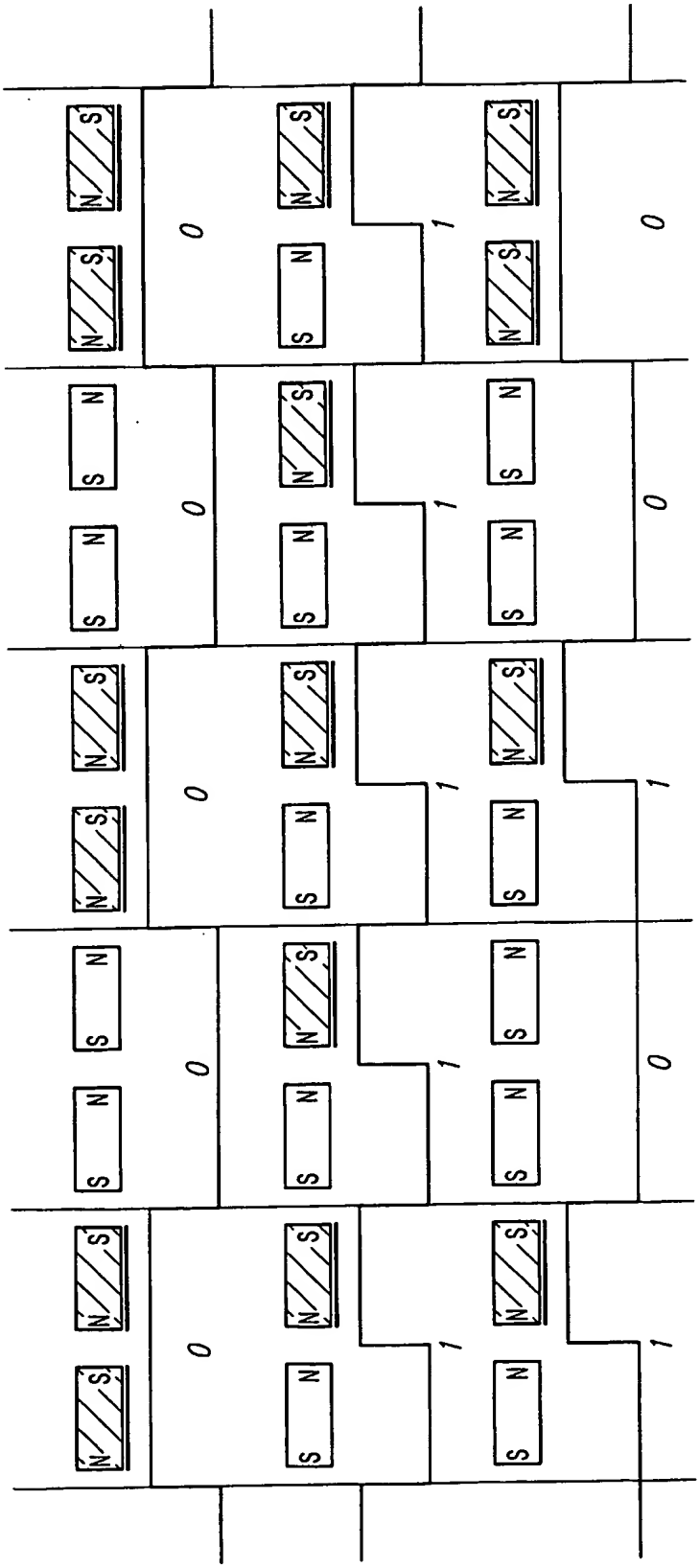


FIG. 7B

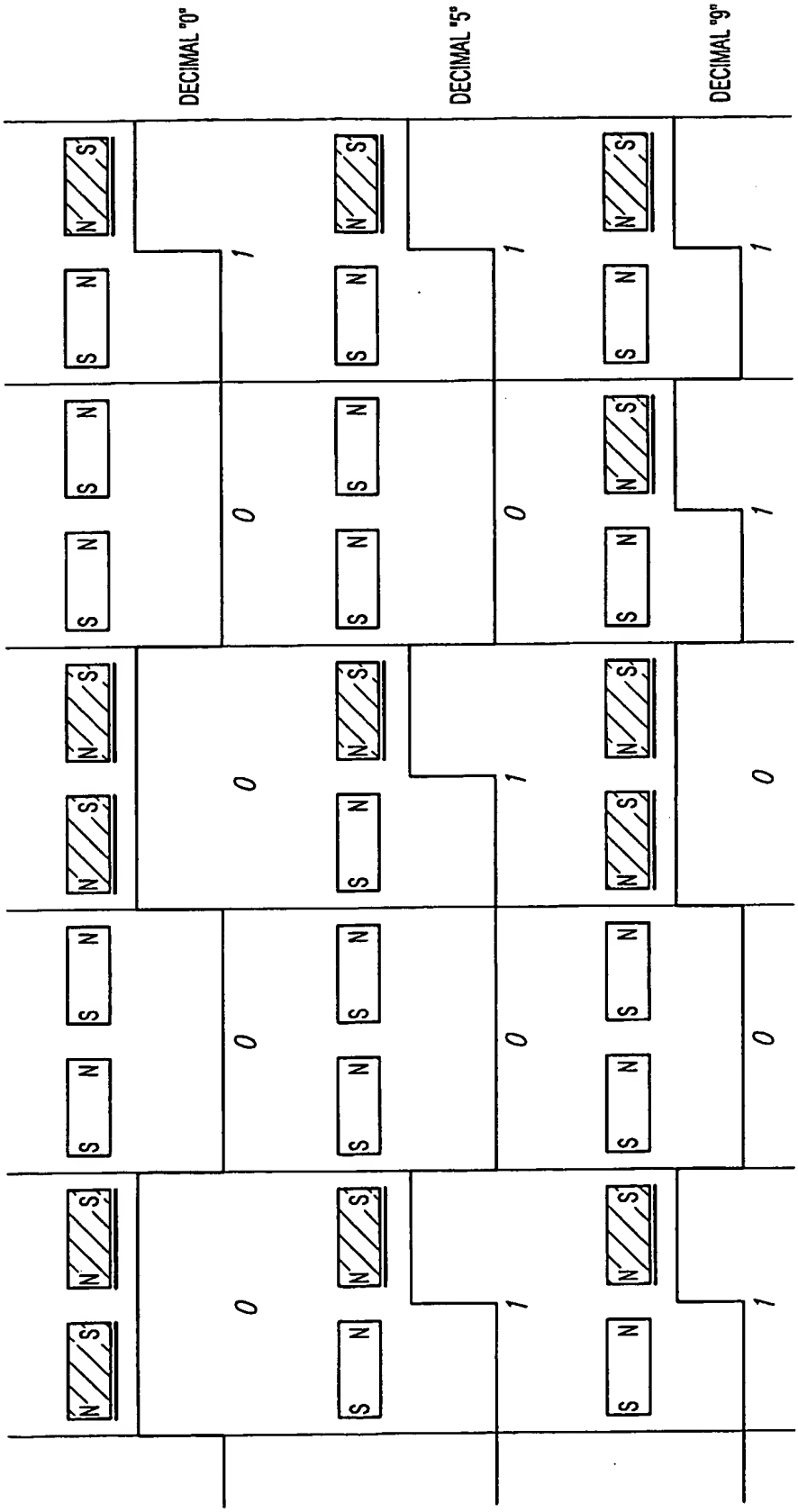


FIG. 7C

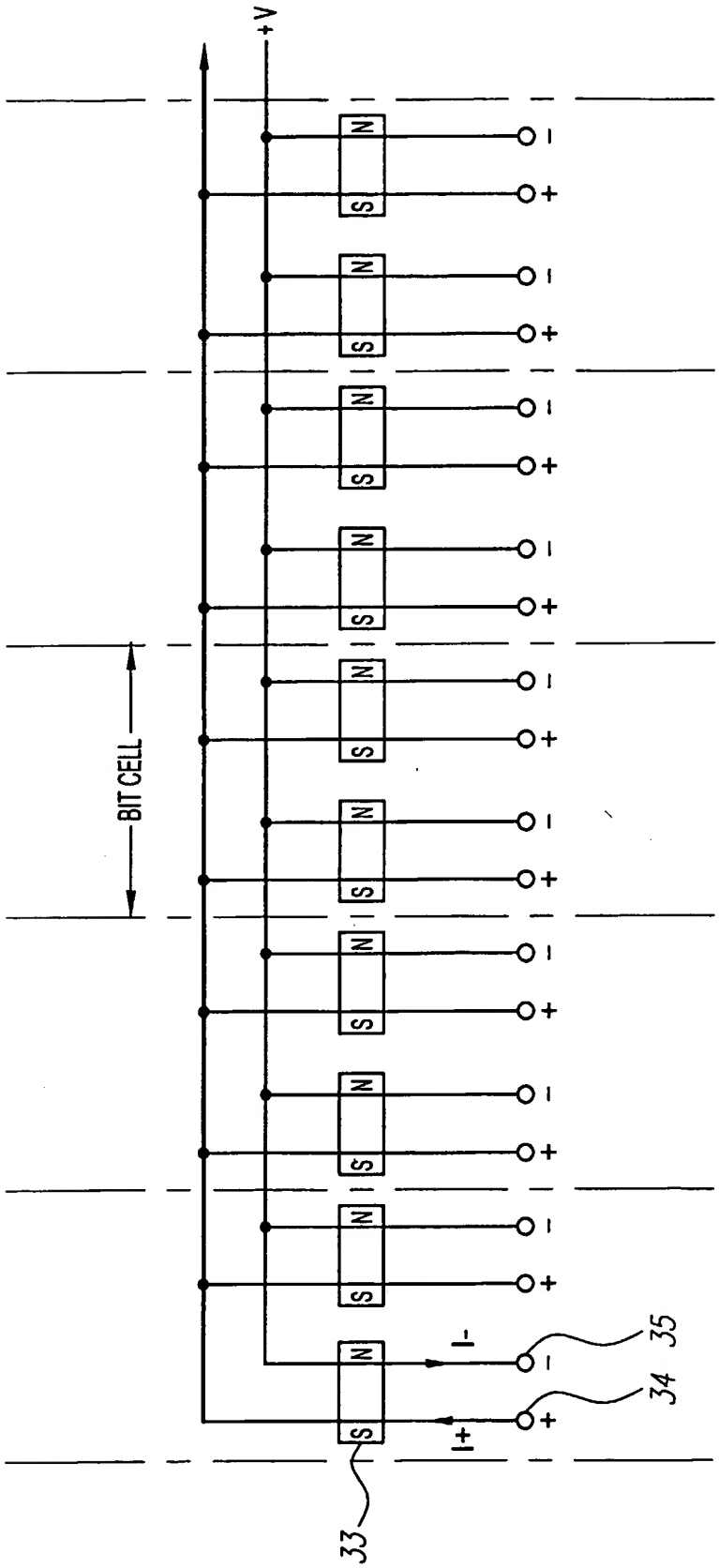


FIG. 7D

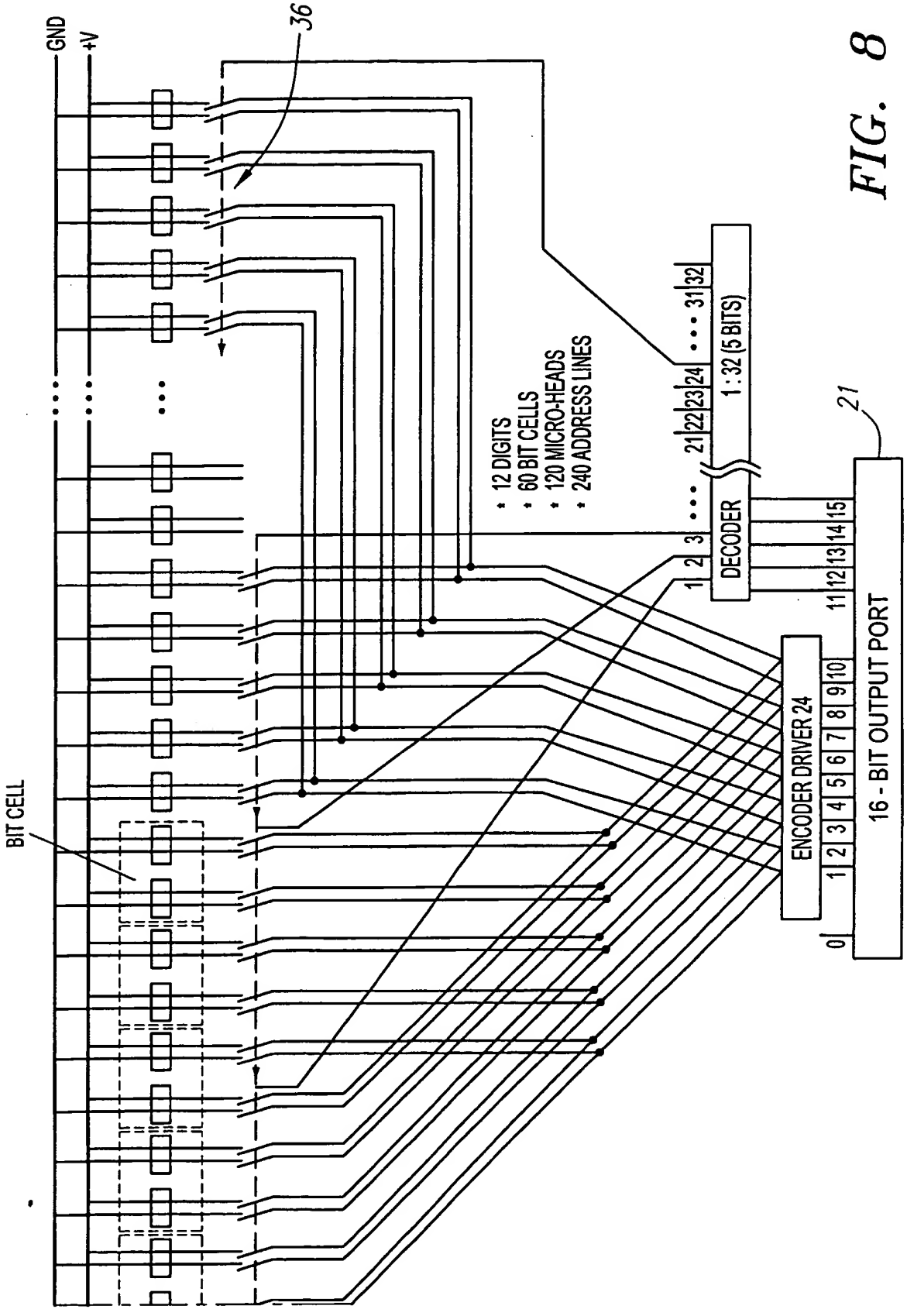

GND
+V
36
BIT CELL
• 12 DIGITS
• 60 BIT CELLS
• 120 MICRO-HEADS
• 240 ADDRESS LINES
1 2 3 • • • 21 22 23 24 • • • 31 32
1:32 (5 BITS)
DECODER
21
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
ENCODER DRIVER 24
0
16 - BIT OUTPUT PORT

FIG. 8

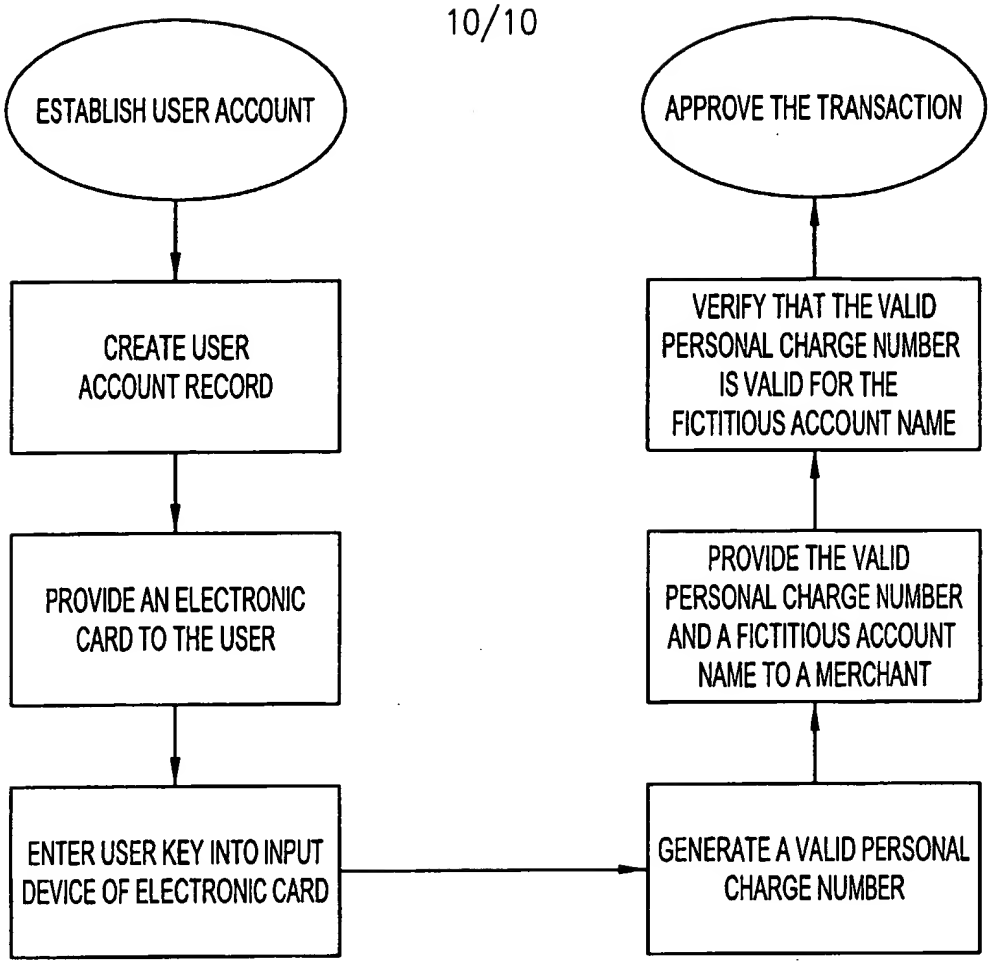

ESTABLISH USER ACCOUNT
CREATE USER ACCOUNT RECORD
PROVIDE AN ELECTRONIC CARD TO THE USER
ENTER USER KEY INTO INPUT DEVICE OF ELECTRONIC CARD
GENERATE A VALID PERSONAL CHARGE NUMBER
PROVIDE THE VALID PERSONAL CHARGE NUMBER AND A FICTITIOUS ACCOUNT NAME TO A MERCHANT
VERIFY THAT THE VALID PERSONAL CHARGE NUMBER IS VALID FOR THE FICTITIOUS ACCOUNT NAME
APPROVE THE TRANSACTION

FIG. 9

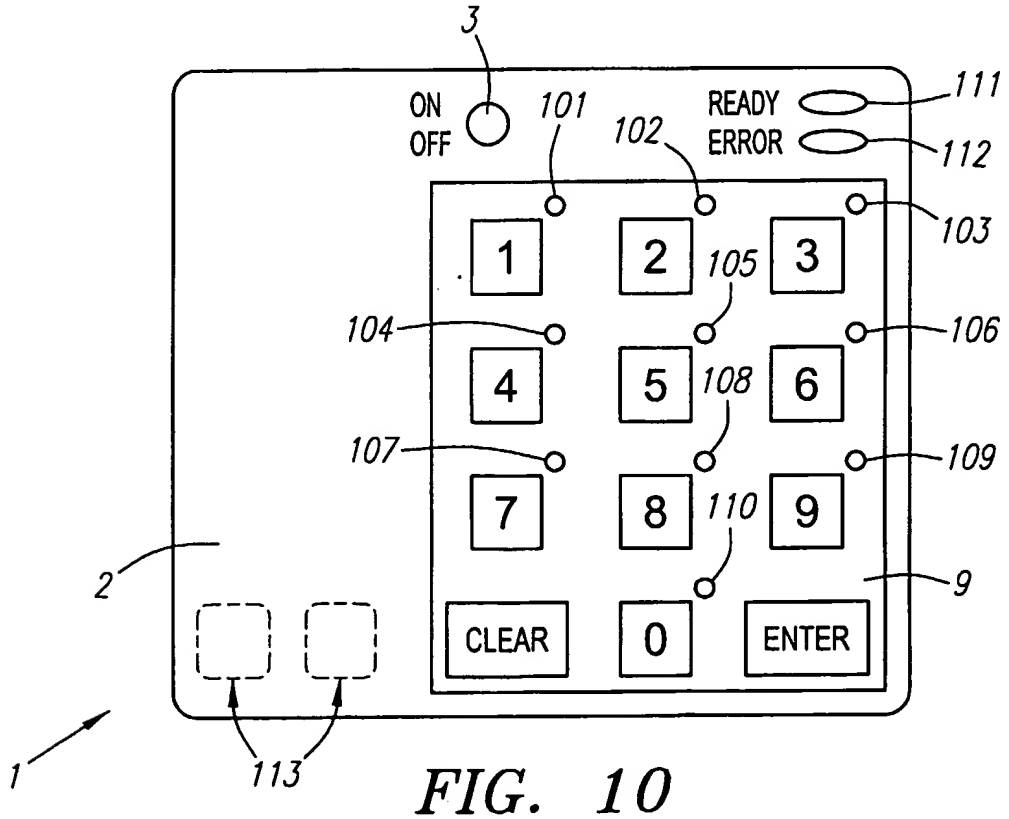

3
ON
OFF
101
102
READY
ERROR
111
112
103
1
2
3
105
104
106
4
5
6
108
107
109
7
8
9
110
2
9
CLEAR
0
ENTER
1
113

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US01/15612

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/00, 17/60; G06K 5/00, 7/01

US CL : 235/375, 379, 380, 382.5; 705/50, 64, 67, 72, 74

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 235/375, 379, 380, 382.5; 705/50, 64, 67, 72, 74

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 4,918,631 A (HARA et al.) 17 April 1990 (17.04.1990), figures 1 and 2 and columns 2-4.	36, 37 --- 16-17, 19-20
Y	US 5,884, 271 A (PITRODA) 16 March 1999 (16.03.1999), figures 1, 3, summary of invention, col. 11, lines 30-57, col. 17, lines 10-44.	3, 7-11, 18-19, 21-35
X, P --- Y, P	US 6,163,771 A (WALKER et al.) 19 December 2000 (19.12.2000), figures 1-3, entire patent.	1-2, 4-6, 12-15, 38-39 --- 3, 7-11, 16-35

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 February 2002 (04.02.2002)	13 FEB 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Larry D Taylor Telephone No. (703) 306-5867

Form PCT/ISA/210 (second sheet) (July 1998)